



D-1154 R2

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In Re Application of:)	
Parmelee, et al.)	
)	Art Unit 2137
Serial No.: 09/683,943)	
)	
Confirm. No.: 5493)	
)	
Filed: March 5, 2002)	Patent Examiner
)	Nadia Khoshnoodi
For: Automated Transaction Machine)	
Digital Signature System And)	
Method)	

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF OF APPELLANTS PURSUANT TO 37 C.F.R. § 41.37

Sir:

The Appellants hereby submit their Appeal Brief pursuant to 37 C.F.R. § 41.37
concerning the above-referenced Application.

10/11/2006 DEMMANU1 00000001 090428 09683943
01 FC:1402 500.00 DA

(i)

REAL PARTY IN INTEREST

The Assignee of all right, title and interest to the above-referenced Application is
Diebold, Incorporated, an Ohio corporation.

(ii) RELATED APPEALS AND INTERFERENCES

The present application and U.S. Application No. 09/683,944 filed March 5, 2002 both claim the benefit under 35 U.S.C. § 119 (e) of U.S. Provisional Application Nos. 60/273,996 filed March 7, 2001 and 60/319,015 filed November 29, 2001. U.S. Application No. 09/683,944 is also on appeal before the Board. Appellants, Appellants' legal representative, and the Assignee of the present application are not aware of any other prior or pending appeals, interferences or judicial proceedings which may be related to, directly affect or have a bearing on the Board's decision in the pending appeal.

(iii)

STATUS OF CLAIMS

Claims 1-41 are pending in the Application.

Claims rejected: 1-41

Claims allowed: none

Claims confirmed: none

Claims withdrawn: none

Claims objected to: none

Claims canceled: none

Appellants appeal the rejections of claims 1-41. These claim rejections were the only claim rejections present in the Office Action (“Action”) dated April 26, 2006. Claims 1-41 have been at least twice rejected.

(iv)

STATUS OF AMENDMENTS

A non-final rejection was made April 26, 2006. No amendments to the claims were requested to be admitted after the non-final rejection.

(v) **SUMMARY OF CLAIMED SUBJECT MATTER**

Concise explanations of exemplary forms of the claimed invention:

With respect to independent claim 1

An exemplary form of the invention is directed to an apparatus. The apparatus comprises at least one computer processor (32, 302, 322) and at least one data store (34) in operative connection with the computer processor (Figure 1; Paragraph [0039]). The at least one data store includes a plurality of digital safe deposit accounts (40) stored therein (Paragraph [0040]). Each of the digital safe deposit accounts is associated with at least one private key (44, 304, 324) (Paragraph [0041]). The computer processor is operative to communicate with a plurality of ATMs (10, 300, 320, 716) (Paragraph [0040]). The computer processor is operative responsive to at least one of the ATMs to cause a digital signature (310, 330) to be produced for an electronic document (42, 162, 306, 326), responsive to the private key associated with one of the digital safe deposit accounts (Figures 9-11; Paragraphs [0039] and [0065] - [0069]).

With respect to independent claim 20

Another exemplary form of the invention is directed to a method that comprises a step (a) of receiving a financial account number (48) from an automated transaction machine (10, 300, 320, 520, 716) (Figure 1; Paragraphs [0047]). The method also comprises step (b) of accessing a private key (44, 304, 324) associated with the financial account number (Figures 9-10; paragraphs [0041], [0047] and [0065] - [0068]). In addition, the method comprises step (c) of enabling an electronic document (42, 162, 306, 326) displayed (612) by the automated

transaction machine, to be digitally signed (618) with the private key (Figures 9-10; paragraphs [0040] - [0041], [0065] - [0068] and [0088] - [0091]).

With respect to independent claim 27

Another exemplary form of the invention is directed to a method that comprises a step (a) of receiving a request from an automated transaction machine (10, 300, 320, 520, 716) to digitally sign (618) an electronic document (42, 162) visually displayed (612) by the automated transaction machine (Figures 1, 9-10, 17; Paragraphs [0040] - [0041], [0065] - [0068] and [0088] - [0091]). The request includes an account number (48) that is associated with a digital safe deposit account (40) (Figures 1 and 2; Paragraphs [0047]). The method also includes step (b) of accessing a private key (44, 324) associated with the digital safe deposit account responsive to the account number. The method includes step (c) of producing a digital signature (330) for the electronic document responsive to the private key (Paragraphs [0041], [0047] and [0065]-[0068]). In addition, the method includes step (d) causing the digital signature to be attached to the electronic document (Paragraphs [0058] and [0065] - [0068]).

With respect to independent claim 31

Another exemplary form of the invention is directed to a method that comprises a step (a) of receiving a request (616) at an ATM (10) to digitally sign (618) an electronic document (42, 162, 306, 326, 346, 406, 426, 446) visually displayed (612) by the ATM (Figures 1, 2, 9-14 and 17; Paragraphs [0065]-[0068] and [0088] - [0091]). The method also includes step (b) of causing a digital signature (310, 330, 350, 410, 430, 450) and a digital time stamp to be produced for the

electronic document (Paragraph [0077]). The method further includes step (c) of causing the digital signature and the digital time stamp to be attached to the electronic document (Paragraphs [0058], [0065] - [0068] and [0077]).

With respect to independent claim 33

Another exemplary form of the invention is directed to a method that comprises a step (a) of receiving with at least one server (10, 300, 320, 716), data associated with a financial account (48) (Figure 1; Paragraphs [0047]). The method also includes step (b) which comprises: responsive to the data associated with the financial account received in (a), causing through operation of the at least one server, a private key (44, 304, 324) which corresponds to the data associated with the financial account received in (a), to be accessed from at least one data store (34) in operative connection with the at least one server. The private key was previously stored in the at least one data store in correlated relation with the data associated with the financial account (Paragraphs [0041], [0047] and [0065] - [0068]). The method further comprises step (c) of causing through operation of the at least one server, a digital signature (310, 330) to be produced for an electronic document (42, 162, 306, 326) responsive to the private key accessed in step (b) (Figures 9-10; Paragraphs [0040] - [0041], [0065] - [0068] and [0088] - [0091]). The method also comprises step (d) of causing through operation of the at least one server, the digital signature to be attached to the electronic document during or after the display (612) of the electronic document through a display device (18, 170) viewable by a customer who is associated with the financial account (Paragraphs [0058]).

(vi) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds to be reviewed in this appeal are:

Whether Appellants' claims 1-6, 8-11, 15-16, 19, 27-30, 33-39, and 41 are obvious under 35 U.S.C. § 103(a) over Wheeler, et al., U.S. publication No. 2002/0026575 ("the Wheeler publication") in view of Cohen, WO 00/55793;

Whether Appellants' claims 7, 12-14, and 40 are obvious under 35 U.S.C. § 103(a) over the Wheeler publication in view of Cohen as applied to claims 1 and 11 and further in view of Randle, et al., U.S. Patent No. 5,974,146 ("Randle");

Whether Appellants' claims 17 and 18 are obvious under 35 U.S.C. § 103(a) over the Wheeler publication in view of Cohen as applied to claim 1 and further in view of Meurer, U.S. publication No. 2004/0215566;

Whether Appellants' claims 20-21, 23, 25-26, and 31-32 are obvious under 35 U.S.C. § 103(a) over the Wheeler publication;

Whether Appellants' claim 22 is obvious under 35 U.S.C. § 103(a) over the Wheeler publication in view of Cohen as applied to claim 20 and further in view of Randle; and

Whether Appellants' claim 24 is obvious under 35 U.S.C. § 103(a) over the Wheeler publication as applied to claim 20 and further in view of Meurer.

Additional Note

The basis on which claim 30 was rejected was not specifically stated in the Action. However, the rejection of claim 30 was discussed on page 12 of the Action. Thus Appellants have assumed that the Action inadvertently omitted claim 30 from the list of claims rejected under 35 U.S.C. § 103(a) over the Wheeler publication in view of Cohen.

If Appellants' assumption regarding the intended rejection of claim 30 is not correct, Appellants reserve the right to respond to any new rejection that may be presented against this claim in the Examiner's Answer.

Further Additional Note

Claims 1-5, 9-11, 13-15, 18, and 31-32 were objected to for reciting the acronym "ATM". Appellants respectfully submit that the meaning of "ATM" is well understood by one of ordinary skill in the art, the term is defined in the specification, and therefore the claims are clear and definite. Nevertheless, Appellants would be willing to amend each independent claim which recites "ATM" to replace the first occurrence of "ATM" with "automated teller machine (ATM)" which is the meaning of the term as disclosed in paragraph [0014] of the present application.

(vii)

ARGUMENT

The Wheeler publication

The Wheeler publication is directed to a method that includes electronically communicating a message over a communications medium regarding an account that is associated with a public key. The corresponding private key of the public key is stored in a device (250) of the account holder such as a card (650). The private key is used to digitally sign the message (Figure 2; Paragraphs [0108]-[0113]).

Cohen

Cohen is directed to a system for electronic commerce including banking tools, products and services (Abstract).

Randle

Randle is directed to a real time bank-centric universal payment system (Column 3, lines 25-28).

Meurer

Meurer is directed to a system for managing ATMs (Abstract).

The 35 U.S.C. § 103 (a) Rejections

The Applicable Legal Standards

Before a claim may be rejected on the basis of obviousness pursuant to 35 U.S.C. § 103, the Patent Office bears the burden of establishing that all the recited features of the claim are

known in the prior art. This is known as *prima facie* obviousness. To establish *prima facie* obviousness, it must be shown that all the elements and relationships recited in the claim are known in the prior art. If the Office does not produce a *prima facie* case, then the Appellants are under no obligation to submit evidence of nonobviousness. MPEP § 2142.

The teaching, suggestion, or motivation to combine the features in prior art references must be clearly and particularly identified in such prior art to support a rejection on the basis of obviousness. It is not sufficient to offer a broad range of sources and make conclusory statements. *In re Dembiczak*, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999).

Even if all of the features recited in the claim are known in the prior art, it is still not proper to reject a claim on the basis of obviousness unless there is a specific teaching, suggestion, or motivation in the prior art to produce the claimed combination. *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561, 1568, 1 U.S.P.Q.2d 1593 (Fed. Cir. 1987). *In re Newell*, 891 F.2d 899, 901, 902, 13 U.S.P.Q.2d 1248, 1250 (Fed. Cir. 1989).

The evidence of record must teach or suggest the recited features. An assertion of basic knowledge and common sense not based on any evidence in the record lacks substantial evidence support. *In re Zurko*, 258 F.3d 1379, 59 U.S.P.Q.2d 1693 (Fed. Cir. 2001).

It is respectfully submitted that the Action does not meet these burdens.

The Wheeler Publication does not qualify as prior art under 35 U.S.C. § 103(a). Therefore all of the rejections of claims 1-41 based on the Wheeler Publication should be reversed

Arguments are presented below for each claim as to why the rejections are improper and should be reversed. In addition to these arguments, Appellants respectfully submit that the

primary reference of the Wheeler publication does not qualify as prior art to the present invention. Therefore on this additional basis, all of the rejections should be reversed.

The present application claims the benefit under 35 U.S.C. § 119 (e) of U.S. Provisional Application Nos. 60/273,996 filed March 7, 2001 and 60/319,015 filed November 29, 2001.

The Wheeler publication was published on February 28, 2002 and corresponds to U.S. Application No. 09/923,179, ("Wheeler application") filed on August 6, 2001. These filing and publication dates are both after Appellants' effective filing date of March 7, 2001.

The Wheeler application is a continuation-in-part of Application No. 09/189,159 filed on November 9, 1998 which is now U.S. Patent No. 6,820,202 ("Wheeler Patent"). The Wheeler application also claims benefit of Provisional Application No. 60/223,076 ("Wheeler provisional") filed on August 4, 2000. However, the specifications of the Wheeler Patent and the Wheeler provisional are not identical to the specification of the Wheeler publication. In particular, the Wheeler provisional has no drawings and includes a written description which does not correspond to the written description in the Wheeler publication. A courtesy copy of the Wheeler provisional is enclosed with this Brief.

The rejections of all of Appellants' claims in the Action were based on citations to one or more of the paragraphs [109], [108-115], [117], [118], [120], [129-132], [145], [170], [172] and [183-190] in the Wheeler publication. However, these paragraphs are not included in the Wheeler provisional. In addition, these paragraphs are also not included in the Wheeler Patent.

The Action has provided a listing (at pages 2-5) which purports to show where the Wheeler provisional supports the Wheeler publication. However, as discussed below in more detail with respect to the independent claims and many of the dependent claims, the portions listed by the Action for the Wheeler provisional do not disclose or suggest all of the features

recited in Appellants' claims against which the Wheeler publication was cited. Therefore the Wheeler provisional does not support the allegedly relevant portions of the Wheeler publication that were cited by the Action to support the rejections of the claims.

The Office has failed to show where each of the features recited in Appellants' claims are disclosed or suggested in the Wheeler provisional. Thus, the portions of the Wheeler publication relied upon in the Action to support the rejections of claims 1- 41 have an effective date of only August 6, 2001 and do not qualify as prior art against Appellants' claims which have an effective filing date for the claimed invention of March 7, 2001. The Office has not addressed let alone established that the portions of the Wheeler publication relied on to support the rejections are entitled to prior art status. It follows that the Office has failed to establish *prima facie* obviousness, and the rejections of claims 1-41 should be reversed.

In addition, a provisional application is required to comply with the first paragraph of 35 U.S.C. § 112 (also Note 35 U.S.C. § 111; 37 C.F.R. § 1.51; and MPEP § 601). It is respectfully submitted that the Wheeler provisional does not meet the requirements of the first paragraph of 35 U.S.C. § 112. The Wheeler provisional does not "contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same . . ."

As can be seen, the Wheeler provisional comprises a combination of four separate (and seemingly unrelated) documents, which based on the headers of each page appear to be e-mail messages. Each of these documents includes numerous topic headings which provide a brief description of some feature or topic. The Wheeler provisional as a whole lacks any description

which indicates how the individual pieces are related, and fails to include any teachings on how these pieces can be used to produce a common system or carry out a common method. The Wheeler provisional contains insufficient disclosure to teach one skilled in the art, at the date of filing, how to make and use the full scope of the alleged invention shown in the Wheeler publication without undue experimentation. Thus the provisional as a whole does not provide an enabling system or method.

The Wheeler publication is not entitled to the August 4, 2000 filing date of the non enabling Wheeler provisional. The Wheeler publication is, at best, only entitled to the August 6, 2001 filing date of the Wheeler application. The application that is the subject of this appeal is entitled to (and claims the benefit of) the March 7, 2001 filing date of provisional application 60/273,996. Thus the Wheeler publication does not constitute prior art against Appellants' invention and all of the rejections should be reversed. For the convenience of the Board, a courtesy copy of the Wheeler provisional is enclosed and is attached at the end of this Brief.

Rejection under 35 U.S.C. § 103(a) over the Wheeler Publication in view of Cohen

In the Action claims 1-6, 8-11, 15-16, 19, 27-30, 33-39, and 41 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Wheeler in view of Cohen. These rejections are respectfully traversed.

Claim 1

Claim 1 is an independent claim which is directed to an apparatus. Claim 1 recites that the apparatus comprises "at least one computer processor; and at least one data store in operative

connection with the computer processor, wherein the at least one data store includes a plurality of digital safe deposit accounts stored therein". Claim 1 also recites that "each of the digital safe deposit accounts is associated with at least one private key". In addition, claim 1 recites that "the computer processor is operative to communicate with a plurality of ATMs". As disclosed at paragraph [0014] of the present application, an "ATM" corresponds to an "automated teller machine". Claim 1 also recites that "the computer processor is operative responsive to at least one of the ATMs to cause a digital signature to be produced for an electronic document responsive to the private key associated with one of the digital safe deposit accounts."

The Wheeler provisional does not support the portions relied on in the Wheeler publication to reject claim 1. Thus the portions of the Wheeler publication relied on to reject claim 1 are not entitled to prior art status with respect to claim 1.

For example, the Action supported the rejection of claim 1 based in part on the discussion at paragraph [0113] of the Wheeler publication. This portion of the Wheeler publication discusses an "account" and "an association between the account and the public key 218". The Action at page 2 states that support for paragraph [0113] is found in the Wheeler provisional at pages 1-3 of the "Aadsstraw" portion and page 6 of the "Rachip" portion. However, neither of these portions discloses or suggests an account or any association between an account and a public key as discussed in paragraph [0113] of the Wheeler provisional. Thus the presumed relevant portions of paragraph [0113] of the Wheeler publication are not supported by the Wheeler provisional and therefore are not prior art with respect to claim 1. The Office has not established *prima facie* obviousness and the rejection of claim 1 should be reversed.

Even if it were somehow possible for the Wheeler provisional to support the Wheeler publication (which it is not), the Wheeler publication and Cohen still do not disclose or suggest all of the features and relationships recited in claim 1. For example, claim 1 recites that each of the accounts is associated with at least one private key. In paragraph [0113], the Wheeler publication teaches away from this recited feature by teaching that Wheeler's account is associated with a public key (not a private key). In the Wheeler publication, the private key is stored on a device (250) of the account holder and is not stored in the account database (214).

A reference teaching away from the recited invention does not support *prima facie* obviousness. It is improper to reconstruct the invention from the disclosure of the Appellants. An obviousness rejection cannot be based on a combination of features in references if making the combination would result in destroying the utility or advantage of the device shown in the prior art references. Note *In re Fine* 5 U.S.P.Q.2d 1598-99 (Fed. Cir. 1988). Neither the Wheeler publication nor Cohen disclose or suggest as recited in claim 1, that "at least one data store includes a plurality of digital safe deposit accounts stored therein" and "each of the digital safe deposit accounts is associated with at least one private key". As the Wheeler publication and Cohen do not disclose or suggest these features, *prima facie* obviousness has not been established, and the rejection of claim 1 should be reversed.

In addition, the Wheeler publication and Cohen also do not disclose or suggest the following features which are explicitly recited in claim 1:

- at least one data store in operative connection with the computer processor, wherein the at least one data store includes a plurality of digital safe deposit accounts stored therein;

- the computer processor is operative to communicate with a plurality of ATMs;
- the computer processor is operative responsive to at least one of the ATMs to cause a digital signature to be produced for an electronic document.

Claim 1 specifically recites "a plurality of digital safe deposit accounts stored" in "at least one data store in operative connection with the computer processor" that communicates with the plurality of ATMs. Nowhere does the Wheeler publication disclose or suggest that its digital signing chip or any other processor, both communicates with a plurality of ATMs and is in operative connection with a data store that includes a plurality of digital safe deposit accounts stored therein.

The Action admits that the Wheeler publication does not disclose a digital safe deposit account. However, the Action asserts that Cohen teaches the use of an electronic safety deposit box at page 12, lines 7-14, and that it would be obvious to modify the method disclosed in the Wheeler publication for the digital account to be a digital safe deposit account. Appellants disagree.

Cohen at page 12, lines 7-14 discusses that an online electronic lockbox is used for storage, access, and record keeping of documents. However, neither Cohen nor the Wheeler publication includes a teaching, suggestion, or motivation to replace the alleged digital account in the Wheeler publication with a digital safe deposit account. Nowhere does Cohen, either at page 12, lines 7-14, or anywhere else in Cohen, provide any specific teaching, suggestion or motivation to modify the alleged digital account of the Wheeler publication to include the features of an online electronic lockbox. The attempts to combine the alleged teachings are clearly nothing more than attempts at hindsight reconstruction of Appellants' claimed invention,

which is legally impermissible and does not constitute a valid basis for a finding of obviousness.

In re Fritch, 22 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Further, as discussed previously, the

"account" discussed in the Wheeler publication is not supported by the Wheeler provisional.

Thus the "account" of the Wheeler publication is not prior art and cannot be replaced with the online electronic lock box discussed in Cohen.

In addition, the alleged combination of the Wheeler publication and Cohen also do not disclose or suggest the following features also recited in claim 1:

- the computer processor is operative responsive to at least one of the ATMs to cause a digital signature to be produced for an electronic document responsive to the private key associated with one of the digital safe deposit accounts.

Nowhere do the applied references disclose or suggest a computer processor that operates responsive to an ATM to digitally sign an electronic document responsive to a private key associated with a digital safe deposit account.

It is not clear, from the Action, which elements in the Wheeler publication the Action regards as corresponding to the features recited in claim 1. In an exemplary embodiment, the recited computer processor in claim 1 corresponds to a server that is operative to communicate with a plurality of ATMs. This server is in operative connection with a data store which includes data corresponding to a plurality of digital safe deposit accounts. Each of the digital safe deposit accounts is associated with a private key. The server operates responsive to an ATM to cause an electronic document to be digitally signed using one of the private keys. The Wheeler publication and Cohen do not disclose or suggest a corresponding apparatus or method.

To reject other claims (such as claim 5), the Action refers to paragraphs [0189] - [0190] of the Wheeler publication. This portion indicates that a card (650) originates a digital signature for a message composed by an ATM (660). Thus it is possible that the Action may regard the recited "computer processor" as corresponding to either the ATM (660) or the card (650) of the Wheeler publication. However, neither the ATM nor the card discussed in the Wheeler publication can correspond to the computer processor recited in claim 1. For example, the ATM of the Wheeler publication cannot correspond to the recited "computer processor", because nowhere does the Wheeler publication disclose or suggest that the ATM (660) includes a "computer processor" that "is operative to communicate with a plurality of ATMs".

In addition, the card of the Wheeler publication cannot correspond to the recited "computer processor", because nowhere does the Wheeler publication disclose or suggest that its card is in operative connection with a data store that "includes a plurality of digital safe deposit accounts stored therein, wherein each of the digital safe deposit accounts is associated with at least one private key". As discussed previously, in the Wheeler publication, accounts are stored in an account database (214), not on a card (650). In the Wheeler publication, the private key is retained in the card (Paragraph [0190]) not in data store comprising a plurality of digital safe deposit accounts.

Also as discussed previously, the Wheeler publication discloses that public keys (not private keys) are associated with the accounts. Thus by teaching that private keys are stored on individual cards or other devices, the Wheeler publication further explicitly teaches away from the apparatus recited in claim 1.

As discussed previously, the portions relied on in Wheeler publication to base the rejection of claim 1, do not qualify as prior art. However, even if the Wheeler publication qualified as prior art (which it does not), Appellants respectfully submit that the Office has not established *prima facie* obviousness with respect to claim 1. The Wheeler publication and Cohen do not disclose or suggest each and every element, feature, and relationship of the claimed invention arranged in the manner recited in the claim, as is required to sustain the rejection. Nor is there any prior art teaching, suggestion, or motivation cited for modifying the Wheeler publication in view of Cohen so as to produce the claimed invention. Further, it would not have been obvious to one having ordinary skill in the art to have modified the Wheeler publication in view of Cohen to have produced the claimed invention.

Appellants respectfully submit that the 35 U.S.C. § 103(a) rejection of claim 1 is improper and should be reversed. It follows that the rejections of claims 2-19 which depend from claim 1 should also be reversed.

Claim 2

Claim 2 depends from claim 1 and recites that the computer processor is operative to receive the electronic document from the at least one ATM, wherein the computer processor is operative to store the electronic document in the data store in association with the one digital safe deposit account. Nowhere do the applied references disclose or suggest these recited features.

The Action admits that the Wheeler publication does not disclose or suggest a computer processor that is operative to receive the electronic document from an ATM, and is also operative to store the electronic document in association with a digital safe deposit account. However, the

Action alleges that this feature would be obvious in view of an alleged teaching at paragraph [0170] in the Wheeler publication that the electronic document may be stored. Appellants disagree.

Paragraph [0170] of the Wheeler publication indicates that data fields in an electronic communication (7601) may be stored. However, where does the Wheeler publication disclose or suggest that such communications are stored in association with a digital safe deposit account as recited in Appellants' claim, or in association with any other type of account? The Action has failed to show where each and every feature recited in the claim is disclosed or suggested in the prior art.

Further, the description relied on in paragraph [0170] of the Wheeler publication for the rejection does not qualify as prior art. The Action alleges (at page 4) that paragraph [0170] of the Wheeler publication is supported by pages 3-6 of the "Aadsstraw" portion of the Wheeler provisional. However, nowhere does this portion of the Wheeler provisional disclose or suggest that the described system stores an electronic document. Thus the asserted portions of paragraph [0170] of the Wheeler publication are not supported by the Wheeler provisional, and therefore are not prior art.

Nowhere does the applied art disclose or suggest an apparatus that stores an electronic document received from an ATM. In addition, nowhere does the applied art disclose or suggest storing an electronic document received from an ATM in a data store in association with an account. Further, nowhere does the applied art disclose or suggest storing an electronic document received from an ATM, in a data store in association with the one digital safe deposit account. In addition, nowhere does the applied art disclose or suggest storing an electronic

document received from an ATM in a data store in association with the one digital safe deposit account, which account is associated with the private key used to sign the electronic document.

The portions relied on in the Wheeler publication to base the rejection do not qualify as prior art. In addition, the Wheeler publication and Cohen do not disclose or suggest each of the features and relationships recited in the claim. Thus, the Office has not established *prima facie* obviousness. On this basis, it is respectfully submitted that the rejection of claim 2 should be reversed.

Claim 3

Claim 3 depends from claim 2 and recites that the computer processor is operative to retrieve the electronic document from the data store and send the electronic document to any one of the plurality of ATMs. Nowhere do the applied references disclose or suggest these recited features.

The Action alleges that Cohen teaches these recited features at page 12, lines 7-14. Appellants disagree. Page 12, lines 7-14 refer to an online electronic lockbox. Nowhere in this description of this online electronic lockbox or anywhere else, does Cohen disclose or suggest a computer processor that is operative to retrieve an electronic document from a data store and send the electronic document to an ATM. The Wheeler publication also does not disclose or suggest these features recited in claim 3.

The Office has not established *prima facie* obviousness with respect to claim 3, and it is respectfully submitted that the rejection should be reversed.

Claim 4

Claim 4 depends from claim 2 and recites that the computer processor is operative to encrypt and decrypt the electronic document stored in the at least one data store responsive to a secret key received from the at least one ATM. Nowhere do the applied references disclose or suggest these recited features.

The Action alleges that the Wheeler publication teaches these features as paragraph [0117]. Appellants disagree. Paragraph [0017] of the Wheeler publication indicates that electronic communication from the account holder (202) may be encrypted. However, nowhere does this portion nor any other portion of the Wheeler publication disclose or suggest a computer processor that is operative to encrypt and decrypt an electronic document stored in a data store responsive to a secret key received from an ATM.

Further, the description relied on in paragraph [0117] of the Wheeler publication as the basis for the rejection, does not qualify as prior art to Appellants' invention. The Action alleges (at page 3) that paragraph [0117] of the Wheeler publication is supported by page 6 of the "Aads" portion and page 1 of the "Aadsstraw" portion of the Wheeler provisional. However, nowhere do these portions of the Wheeler provisional disclose that electronic communication from the account holder (202) is encrypted. Thus the allegedly relevant portions of paragraph [0117] of the Wheeler publication are not supported by the Wheeler provisional. In addition, nowhere does the Wheeler provisional disclose or suggest that a computer processor is operative to encrypt and decrypt an electronic document stored in a data store responsive to a secret key received from the an ATM. Cohen also does not disclose or suggest these features recited in claim 4.

The Office has not established *prima facie* obviousness with respect to claim 4, and it is respectfully submitted that the rejection should be reversed.

Claim 5

Claim 5 depends from claim 1 and recites that each digital safe deposit account is associated with a financial account number. In addition, claim 5 recites that the computer processor is operative to access the private key associated with the one digital safe deposit account responsive to a message received from the at least one ATM, which message includes a financial account number that corresponds to the financial account number associated with the one digital safe deposit account. Nowhere do the applied references disclose or suggest these recited features.

The Action alleges that the Wheeler publication teaches these features in paragraphs [0189] - [0190]. Appellants disagree. This portion of the Wheeler publication indicates that an electronic message generated by an ATM (660) includes an account number (716). This message is transmitted to a card (650) for digitally signing by the card using a private key retained in the card. However, as discussed previously with respect to claim 1, neither the ATM (660) nor the card (650) discussed in paragraphs [0189] - [0190] of the Wheeler publication can correspond to the recited computer processor. Thus nowhere does this portion or any other portion of the Wheeler publication disclose or suggest a computer processor (as recited in claim 1) that is operative to access a private key associated with a digital safe deposit account, responsive to a message received from an ATM. Further, nowhere does the Wheeler publication disclose or suggest that the computer processor (as recited in claim 1) is operative to access the private key

associated with the one digital safe deposit account responsive to a message received from the at least one ATM which includes a financial account number that corresponds to the financial account number associated with the one digital safe deposit account.

Further, the description relied on by the Action in paragraphs [0189] - [0190] of the Wheeler publication, as the basis for the rejection, does not qualify as prior art. The Action alleges (at page 5) that paragraphs [0189] - [0190] of the Wheeler publication are supported by pages 1 and 6 of the "Aadsstraw" portion and pages 1-2 of the "Aadsbrnd" portion of the Wheeler provisional. However, nowhere do these portions of the Wheeler provisional disclose an electronic message including an account number which is transmitted to a card by an ATM for digitally signing by the card using a private key retained in the card.

Thus the presumed relevant portions of paragraphs [0189] - [0190] of the Wheeler publication are not supported by the Wheeler provisional. In addition, nowhere else does the Wheeler provisional disclose or suggest the features recited in claim 5. Further, Cohen also does not disclose or suggest the features recited in claim 5.

The Office has not established *prima facie* obviousness with respect to claim 5, and it is respectfully submitted that the rejection should be reversed.

Claim 6

Claim 6 depends from claim 5 and recites that the at least one financial account number corresponds to a credit card number. Nowhere do the applied references disclose or suggest this recited feature.

The Action refers to paragraph [0183] of the Wheeler publication to support the rejection of claim 6. Although paragraph [0183] discusses a card (650) that may be a credit card, neither this portion nor any other portion of the Wheeler publication, discloses or suggests an apparatus that uses a credit card number as recited in the claim. For example, nowhere does the Wheeler publication disclose or suggest the computer processor (as recited in claim 1) is operative to access the private key associated with the one digital safe deposit account responsive to a message received from the at least one ATM, which message includes a credit card number that corresponds to the financial account number associated with the one digital safe deposit account. In addition, Cohen also does not disclose or suggest the features recited in claim 6.

The Office has not established *prima facie* obviousness with respect to claim 6, and it is respectfully submitted that the rejection should be reversed.

Claim 8

Claim 8 depends from claim 1 and recites that the computer processor is operative to maintain and store in the at least one data store, an access log in association with each digital safe deposit account. Nowhere do the applied references disclose or suggest this recited feature.

For example, nowhere does paragraph [0120] of the Wheeler publication disclose or suggest an access log as alleged in the Action. Further, nowhere do the Wheeler publication and Cohen disclose or suggest a computer processor which is operative to maintain and store in the at least one data store, an access log in association with each digital safe deposit account.

The Office has not established *prima facie* obviousness with respect to claim 8, and it is respectfully submitted that the rejection should be reversed.

Claim 9

Claim 9 depends from claim 1 and recites that the at least one ATM includes a cash dispenser, wherein the computer processor is operative through communication with a financial transaction processing system to cause a dispense of cash from the cash dispenser to be authorized.

Nowhere do the applied references disclose or suggest a computer processor that is operative responsive to at least one of the ATMs to cause a digital signature to be produced and that is also operative to cause a dispense of cash from the cash dispenser of the at least one ATM to be authorized.

The Office has not established *prima facie* obviousness with respect to claim 9, and it is respectfully submitted that the rejection should be reversed.

Claim 10

Claim 10 depends from claim 1 and recites that the computer processor is operative to cause a new digital safe deposit account to be created in the data store responsive to communication from the at least one ATM. Nowhere do the applied references disclose or suggest this recited feature.

The Action refers to paragraphs [0129] - [0132] of the Wheeler publication with respect to the features recited in claim 10. These portions discuss a method of establishing a new Account Based Digital Signature (ABDS) account. An ABDS account does not correspond to the recited digital safe deposit accounts. For example, nowhere to the applied references disclose or suggest a digital safe deposit account that is associated with a private key. In addition,

nowhere do the Wheeler publication or Cohen disclose or suggest creating a new ABDS account responsive to communication from an ATM. Further, the applied references do not disclose or suggest creating a new digital safe deposit account in a data store responsive to communication from an ATM.

The Office has not established *prima facie* obviousness with respect to claim 10, and it is respectfully submitted that the rejection should be reversed.

Claim 11

Claim 11 depends from claim 10 and recites that the computer processor is operative to cause a new private key and a corresponding public key to be produced responsive to communication from the at least one ATM. Claim 11 further recites that the computer processor is operative to store the private key in association with the new digital safe deposit account. Nowhere do the applied references disclose or suggest these recited features.

The Action refers to paragraphs [0108] - [0113] of the Wheeler publication with respect to the features recited in claim 11. These portions discuss the overall structure of an ABDS system. However, these portions of the Wheeler publication do not disclose or suggest a computer processor that is operative to cause a new private key and a corresponding public key to be produced responsive to communication from the at least one ATM. Cohen also does not disclose or suggest these features.

In addition, as discussed previously, the Wheeler publication teaches associating the public key (not the private key) with its account. Nowhere does the applied art disclose or suggest storing the private key in association with the new digital safe deposit account.

The Office has not established *prima facie* obviousness with respect to claim 11, and it is respectfully submitted that the rejection should be reversed.

Claim 15

Claim 15 depends from claim 1 and recites that the computer processor is operative to receive a one-way hash of the electronic document from the at least one ATM. Claim 15 also recites that the computer processor is operative to cause the digital signature to be generated responsive to the one-way hash and the private key. Nowhere do the applied references disclose or suggest these recited features.

The Action alleges that paragraph [00145] of the Wheeler publication discloses these features. Appellants disagree. This portion of the Wheeler publication indicates that a device originates a digital signature for an electronic message using the private key stored in the device. This portion also indicates that the device performs the hash function on the message. Consequently, such a device cannot correspond to the computer processor recited in the claim. Nowhere do the Wheeler publication or Cohen disclose or suggest a computer processor that is operative to receive a one-way hash of an electronic document from an ATM, and then generate a digital signature responsive to the received one-way hash and a private key.

The Office has not established *prima facie* obviousness with respect to claim 15, and it is respectfully submitted that the rejection should be reversed.

Claim 16

Claim 16 depends from claim 1 and recites that the computer processor is operative to cause a second digital signature to be produced for the electronic document responsive to a private key that is not associated with the one digital safe deposit account. Nowhere do the applied references disclose or suggest these recited features.

Paragraph [0118] of the Wheeler publication indicates that an account (285) has associated therewith a plurality of different customer or account holders, each of whom has a different public key for accessing the account. This portion of the Wheeler publication discloses plural public keys (not private keys) associated with an account. Further, this portion of the Wheeler publication discloses that the plural public keys are used for accessing the account (not digitally signing an electronic document). Nowhere in this portion of the Wheeler publication, is there disclosed or suggested a computer processor that is operative to cause two digital signatures to be produced for an electronic document. Further, nowhere do the applied references disclose or suggest a computer processor that is operative to produce a first digital signature for an electronic document responsive to a private key associated with a digital safe deposit account, and that is operative to produce a second digital signature for the same electronic document responsive to a private key that is not associated with the digital safe deposit account.

The Office has not established *prima facie* obviousness with respect to claim 16, and it is respectfully submitted that the rejection should be reversed.

Claim 19

Claim 19 depends from claim 1 and recites that the computer processor is operative to cause a digital time stamp to be produced and attached to the electronic document.

The Action alleges that this feature is disclosed in the Wheeler publication at paragraph [0172]. However, the description relied on in paragraphs [0172] of the Wheeler publication to base the rejection, does not qualify as prior art. The Action alleges (at page 4) that paragraph [0172] of the Wheeler publication is supported by page 6 of the "Aadsstraw" portion of the Wheeler provisional. However, this portion only states that a unique message includes a "data/time". Nowhere does the Wheeler provisional disclose or suggest a computer processor that is operative to cause a "digital time stamp" to be produced and attached to an electronic document. Thus the portion of the Wheeler publication used as a basis to reject the claim does not qualify as prior art.

The Office has not established *prima facie* obviousness with respect to claim 19, and it is respectfully submitted that the rejection should be reversed.

Claim 27

Claim 27 is an independent claim which is directed to a method. The method comprises:

- (a) receiving a request from an automated transaction machine to digitally sign an electronic document visually displayed by the automated transaction machine, wherein the request includes an account number that is associated with a digital safe deposit account;
- (b) accessing a private key associated with the digital safe deposit account responsive to the account number;
- (c) producing a digital signature for the electronic document responsive to the private key; and

(d) causing the digital signature to be attached to the electronic document.

The Wheeler provisional does not support the portions relied on in the Wheeler publication to reject claim 27. Thus the portions of the Wheeler publication relied on to reject claim 27 are not entitled to prior art status with respect to claim 27.

For example, the Action based rejection of claim 27 on paragraph [0190] of the Wheeler publication. Paragraph [0190] of the Wheeler publication discusses that a message generated by an ATM is transmitted to a card (650) for digitally signing by a card using a private key stored in the card. The Action alleges (at page 5) that paragraph [0190] of the Wheeler publication is supported by pages 1-2 of the "Aadsbrnd" portion of the Wheeler provisional. However, nowhere do these portions of the Wheeler provisional disclose an electronic message which is transmitted to a card by an ATM for digitally signing by the card using a private key retained in the card. Thus the asserted relevant portions of paragraph [0190] of the Wheeler publication are not supported by the Wheeler provisional, and therefore are not prior art with respect to claim 27. The Office has not established *prima facie* obviousness, and the rejection of claim 27 should be reversed.

In addition, even if it were somehow possible for the Wheeler provisional to support the Wheeler publication (which it is not), the Wheeler publication and Cohen still do not disclose or suggest all of the features and relationships recited in claim 27. For example, nowhere do the applied references disclose or suggest:

- receiving a request from an automated transaction machine to digitally sign an electronic document visually displayed by the automated transaction machine,

- wherein the request includes an account number that is associated with a digital safe deposit account;
- accessing a private key associated with the digital safe deposit account responsive to the account number;
- producing a digital signature for the electronic document visually displayed by the automated transaction machine; or
- causing the digital signature to be attached to the electronic document visually displayed by the automated transaction machine.

Although the Action does not state which elements of Wheeler correspond to respective elements recited in claim 27, it appears that the Office may regard the card discussed in paragraph [0190] as corresponding to an element which carries out steps (a) through (d) of claim 27. However, Appellants respectfully submit that nowhere does Wheeler disclose or suggest that these steps are carried out by the described card nor any other device described in the Wheeler publication. In addition, Cohen also does not disclose or suggest these recited steps.

For example, with respect to step (a), nowhere does the Wheeler publication or Cohen disclose or suggest receiving a request from an automated transaction machine to digitally sign an electronic document visually displayed by the automated transaction machine. Nowhere does the Wheeler publication disclose or suggest that the electronic message transmitted by the ATM (660) to the card (650) is ever visually displayed by ATM.

In addition, with respect to step (b), nowhere does the Wheeler publication or Cohen disclose or suggest accessing a private key associated with the digital safe deposit account

responsive to the account number. Although paragraph [0189] indicates that the message transmitted by the ATM may include an account number therein, nowhere does the Wheeler publication disclose or suggest that the card (650) accesses the private key retained therein responsive to the account number.

Further, with respect to step (c), nowhere does the Wheeler publication or Cohen disclose or suggest producing a digital signature for the electronic document visually displayed by the automated transaction machine. Also, with respect to step (d), nowhere does the Wheeler publication or Cohen disclose or suggest causing the digital signature to be attached to the electronic document visually displayed by the automated transaction machine.

In addition, the Action admits that the Wheeler publication does not disclose a digital safe deposit account. However, the Action asserts that Cohen teaches the use of an electronic safety deposit box at page 12, lines 7-14, and that it would be obvious to modify the method disclosed in the Wheeler publication for the digital account to be a digital safe deposit account. Appellants disagree.

Cohen at page 12, lines 7-14 discusses that an online electronic lockbox is used for storage, access, and record keeping of documents. However, neither Cohen nor the Wheeler publication includes a teaching, suggestion, or motivation to replace the alleged digital account in the Wheeler publication with a digital safe deposit account. Nowhere does Cohen, either at page 12, lines 7-14, or anywhere, provide a specific teaching, suggestion or motivation to modify the alleged digital account of the Wheeler publication to include the features of an online electronic lockbox. The attempts to combine the alleged teachings are clearly nothing more than attempts at hindsight reconstruction of Appellants' claimed invention, which is legally impermissible and

does not constitute a valid basis for a finding of obviousness. *In re Fritch*, 22 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Further, as discussed previously, the "account" discussed in the Wheeler publication is not supported by the Wheeler provisional. Thus the "account" of the Wheeler publication is not prior art to Appellants' invention and cannot be replaced with the online electronic lock box discussed in Cohen as a valid basis for rejection.

As discussed previously, the portions relied on in the Wheeler publication as the basis for the rejection of claim 27, do not qualify as prior art. In addition, even if the Wheeler publication qualified as prior art (which it does not), Appellants respectfully submit that the Office has not *established prima facie* obviousness with respect to claim 27. The Wheeler publication and Cohen do not disclose or suggest each and every element, feature, relationship and step of the claimed invention arranged in the manner recited in the claim, as is required to sustain the rejection. Nor is there any prior art teaching, suggestion, or motivation cited for modifying the Wheeler publication in view of Cohen so as to produce the claimed invention. Further, it would not have been obvious to one having ordinary skill in the art to have modified the Wheeler publication in view of Cohen to have produced the claimed invention. Appellants respectfully submit that the 35 U.S.C. § 103(a) rejection of claim 27 is improper and should be reversed. It follows that the rejections of claims 28-30 which depend from claim 27 should also be reversed.

Claim 28

Claim 28 depends from claim 27 and recites that the method further comprises step (e) of storing a digitally signed copy of the electronic document in a data store in association with the

digital safe deposit account computer. Nowhere do the applied references disclose or suggest this recited step.

The Action refers to paragraph [0170] of the Wheeler publication to support the rejection of claim 28. Paragraph [0170] of the Wheeler publication indicates that data fields in an electronic communication (7601) may be stored. However, where does the Wheeler publication disclose or suggest that such communications are stored in association with a digital safe deposit account as recited, or with any other type of account? The Action has failed to show where each and every feature recited in the claim is disclosed or suggested in the prior art.

Further, the description relied on in paragraph [0170] of the Wheeler publication as the asserted basis for the rejection does not qualify as prior art. The Action alleges (at page 4) that paragraph [0170] of the Wheeler publication is supported by pages 3-6 of the "Aadsstraw" portion of the Wheeler provisional. However, nowhere does this portion disclose or suggest that the described system stores an electronic document. Thus the asserted relevant portions in paragraph [0170] of the Wheeler publication are not supported by the Wheeler provisional, and therefore are not prior art.

Further, nowhere does the applied art disclose or suggest a method that stores an electronic document that was visually displayed by an automated transaction machine. Also, nowhere does the applied art disclose or suggest storing an electronic document visually displayed by an automated transaction machine, in a data store in association with an account. Nowhere does the applied art disclose or suggest storing an electronic document visually displayed by an automated transaction machine, in a data store in association with the one digital safe deposit account. In addition, nowhere does the applied art disclose or suggest storing an

electronic document visually displayed by an automated transaction machine, in a data store in association with a digital safe deposit account, which account is associated with the private key used to sign the electronic document.

The portions relied on in the Wheeler publication to base the rejection do not qualify as prior art. In addition, the Wheeler publication and Cohen do not disclose or suggest each of the features, relationships, and steps recited in the claim. Thus, the Office has not established *prima facie* obviousness. On this basis, it is respectfully submitted that the rejection of claim 28 should be reversed.

Claim 29

Claim 29 depends from claim 27 and recites that in step (a) the account number corresponds to a financial account number. Nowhere do the applied references disclose or suggest this recited step.

The Action refers to paragraph [0183] of the Wheeler publication to support the rejection of claim 29. Although paragraph [0183] discusses a card (650) that may be a credit card, neither this portion nor any other portion of the Wheeler publication discloses or suggests a method that involves use of a financial account number as recited. For example, nowhere does the Wheeler publication disclose or suggest a step of accessing a private key associated with the digital safe deposit account responsive to a financial account number. In addition, Cohen also does not disclose or suggest this recited step.

The Office has not established *prima facie* obviousness with respect to claim 29, and it is respectfully submitted that the rejection should be reversed.

Claim 30

Claim 30 depends from claim 27 and recites that the method comprises (e) dispensing cash from the automated transaction machine. Nowhere do the applied references disclose both dispensing cash from an automated transaction machine and receiving a request from the same automated transaction machine to digitally sign an electronic document visually displayed by the automated transaction machine.

The Office has not established *prima facie* obviousness with respect to claim 30, and it is respectfully submitted that the rejection should be reversed.

Claim 33

Claim 33 is an independent claim which is directed to a method. The method comprises: (a) receiving with at least one server, data associated with a financial account. The method also comprises: (b) responsive to the data associated with the financial account received in (a), causing through operation of the at least one server, a private key which corresponds to the data associated with the financial account received in (a), to be accessed from at least one data store in operative connection with the at least one server. The private key was previously stored in the at least one data store in correlated relation with the data associated with the financial account. In addition, the method comprises: (c) causing through operation of the at least one server, a digital signature to be produced for an electronic document responsive to the private key accessed in (b); and (d) causing through operation of the at least one server, the digital signature to be attached to the electronic document during or after the display of the electronic document through a display device viewable by a customer associated with the financial account.

The Wheeler provisional does not support the portions in the Wheeler publication relied on by the Action to reject claim 33. Thus the portions of the Wheeler publication relied on to reject claim 33 are not entitled to prior art status with respect to claim 33.

For example, the Action supported the rejection of claim 33 based on paragraph [0190] of the Wheeler publication. Paragraph [0190] discusses that a message generated by an ATM is transmitted to a card (650) for digitally signing by a card using a private key stored in the card. The Action alleges (at page 5) that paragraph [0190] of the Wheeler publication is supported by pages 1-2 of the "Aadsbrnd" portion of the Wheeler provisional. However, nowhere do these portions of the Wheeler provisional disclose an electronic message which is transmitted to a card by an ATM for digitally signing by the card using a private key retained in the card. Thus the presumed relevant portions of paragraph [0190] of the Wheeler publication are not supported by the Wheeler provisional, and therefore are not prior art with respect to claim 33. The Office has not established *prima facie* obviousness, and the rejection of claim 33 should be reversed.

In addition, even if it were somehow possible for the Wheeler provisional to support the Wheeler publication, the Wheeler publication and Cohen still do not disclose or suggest all of the features and relationships recited in claim 33. For example, nowhere do the applied references disclose or suggest:

- responsive to the data associated with the financial account received [by at least one server] in (a), causing through operation of the at least one server, a private key which corresponds to the data associated with the financial account received in (a) to be accessed from at least one data store in operative connection with the at least one server,

- wherein the private key was previously stored in the at least one data store in correlated relation with the data associated with the financial account;
- causing through operation of the at least one server, a digital signature to be produced for an electronic document responsive to the private key accessed;
- causing through operation of the at least one server, the digital signature to be attached to the electronic document during or after the display of the electronic document through a display device viewable by a customer associated with the financial account.

The Action admits that the Wheeler publication does not disclose a server that carries out the recited steps. However, the Action appears to be arguing that the Wheeler publication discloses a smart card with a processor that carries out the steps recited in claim 33 and that it would be obvious to carry out these steps on a server instead of a smart card based on the suggestion in Cohen at page 16, line 32 to page 17, line 5. Appellants disagree.

First of all, the card (650) discussed in paragraph [0190] of the Wheeler publication does not carry out each of the steps recited in claim 33. Further, the discussion in the referenced portion of Cohen does not provide any teaching, suggestion, or motivation to modify Wheeler to replace the card of the Wheeler publication with a server. In addition, even if it were possible (which it is not) for the Wheeler publication to be modified by Cohen as suggested in the Action,

such a combination would still not disclose or suggest each of the features, relationships, and steps recited in claim 33.

For example, in the Wheeler publication, a private key is stored in the card (650), not in a server. Nowhere does the Wheeler publication disclose or suggest that its described private key is ever stored in the at least one data store of a server in correlated relation with the data associated with the financial account. Rather, the Wheeler publication teaches the exact opposite by teaching that the public keys are stored in the account database (not the private keys).

Thus the applied art does not disclose or suggest a step of causing through operation of a server responsive to data associated with a financial account, a private key which corresponds to the data associated with a financial account to be accessed from at least one data store in operative connection with the server. In addition, nowhere do the applied references disclose or suggest that the private key is previously stored in the at least one data store in correlated relation with the data associated with the financial account.

Further, Cohen at page 16, line 32, to page 17, line 5, does not provide any motivation to modify the card of the Wheeler publication to correspond to a server. This referenced portion of Cohen discusses that a consumer can maintain his or her own webbank on a server. Such a webbank corresponds to a web page that can be used to engage in financial transactions. However, nowhere in this portion, or anywhere else does Cohen suggest that the system described in the Wheeler publication should be configured in an opposite manner, by having private keys be stored in a data store of a server rather than in the individual cards of the users as specifically taught.

An obviousness rejection cannot be based on a combination of features in references if making the combination would result in destroying the utility or advantage of the device shown in the prior art references. *In re Fine*, 5 U.S.P.Q.2d 1598-99 (Fed. Cir. 1988). As the combination of features asserted in the Action would destroy the utility and advantages of the cited reference, it is respectfully submitted that the rejection is improper and should be reversed.

In addition, nowhere do the applied references disclose other features, relationships and steps recited in claim 33. For example, nowhere do the applied references disclose or suggest causing through operation of a server (or a card), a digital signature to be produced for an electronic document responsive to a private key accessed responsive to data associated with the financial account.

Further, the Action admits that the Wheeler publication does not disclose or suggest causing through operation of the server, the digital signature to be attached to the electronic document during or after the display of the electronic document through a display device viewable by a customer associated with the financial account. However, the Action asserts that it would be obvious to modify the method disclosed in the Wheeler publication to also visually display the message with the attached signature based on paragraphs [0188] - [0189] of the Wheeler publication. Appellants disagree.

In paragraph [0189], the Wheeler publication indicates that the ATM (660) displays a menu of operations which include money withdrawal, balance inquiry, statement request, money transfer, money deposit, bill payment. Such a menu displayed by an ATM does not disclose or inherently require a message to be displayed by the ATM which has been or will be digitally signed. The message transmitted from the ATM that is signed by the card in the Wheeler

publication, corresponds to an instruction to the financial institution corresponding to the desired operation of the account holder (paragraph [0189]). Nowhere does the Wheeler publication disclose or suggest that such a message is ever displayed by the ATM. Nor would displaying such a message be inherent in the Wheeler publication, as such a message could be transferred from the ATM to a financial institution without an need for a user to view it at the ATM.

Anticipation by inherency requires that the Patent Office establish that persons skilled in the art would recognize that the missing element is necessarily present in the reference. To establish inherency the Office must prove through citation to prior art that the feature alleged to be inherent is "necessarily present" in a cited reference. Inherency may not be established based on probabilities or possibilities. It is plainly improper to reject a claim on the basis of 35 U.S.C. § 102 based merely on the possibility that a particular prior art disclosure could or might be used or operated in the manner recited in the claim. *In re Robertson*, 169 F.3d 743, 49 U.S.P.Q.2d 1949 (Fed. Cir. 1999).

Nowhere does the applied art explicitly or inherently disclose or suggest causing through operation of the at least one server, the digital signature to be attached to the electronic document during or after the display of the electronic document through a display device viewable by a customer associated with the financial account.

As discussed previously, the portions relied on in the Wheeler publication as the basis for the rejection of claim 33, do not qualify as prior art. In addition, even if the Wheeler publication qualified as prior art (which it does not), Appellants respectfully submit that the Office has not *established prima facie* obviousness with respect to claim 33. The Wheeler publication and Cohen do not disclose or suggest each and every element, feature, relationship and step of the

claimed invention arranged in the manner recited in the claim, as is required to sustain the rejection. Nor is there any prior art teaching, suggestion, or motivation cited for modifying the Wheeler publication in view of Cohen so as to produce the claimed invention. Further, it would not have been obvious to one having ordinary skill in the art to have modified the Wheeler publication in view of Cohen to have produced the claimed invention.

Appellants respectfully submit that the 35 U.S.C. § 103(a) rejection of claim 33 is improper and should be reversed. It follows that the rejections of claims 34-41 which depend from claim 33 should also be reversed.

Claim 34

Claim 34 depends from claim 33 and recites that in step (a) the data associated with the financial account is representative of a financial account number. Nowhere do the applied references disclose or suggest this recited step.

The Action refers to paragraph [0183] of the Wheeler publication to support the rejection of claim 34. Although paragraph [0183] discusses a card (650) that may be a credit card, neither this portion nor any other portion of the Wheeler publication discloses or suggests a method that involves use of a financial account number as recited. For example, nowhere does the Wheeler publication disclose or suggest a step of causing through operation of the at least one server responsive to data associated with a financial account number, a private key which corresponds to the data to be accessed from at least one data store in operative connection with the at least one server. In addition, Cohen also do not disclose or suggest this recited step.

The Office has not established *prima facie* obviousness with respect to claim 34, and it is respectfully submitted that the rejection should be reversed.

Claim 35

Claim 35 depends from claim 34 and recites that in step (a) the at least one financial account number corresponds to at least one of a credit card number, a debit card number, and a bank account number. Nowhere do the applied references disclose or suggest this recited step.

The Action refers to paragraph [0183] of the Wheeler publication to support the rejection of claim 35. Although paragraph [0183] discusses a card (650) that may be a credit card, neither this portion nor any other portion of the Wheeler publication discloses or suggests a method that involves use of a credit card number as recited. For example, nowhere does the Wheeler publication disclose or suggest a step of causing through operation of the at least one server responsive to data associated with at least one of a credit card number, a debit card number, and a bank account number, a private key which corresponds to the data to be accessed from at least one data store in operative connection with the at least one server. In addition, Cohen also does not disclose or suggest this recited step.

The Office has not established *prima facie* obviousness with respect to claim 35, and it is respectfully submitted that the rejection should be reversed.

Claim 36

Claim 36 depends from claim 34 and recites that in (a) the data representative of the financial account number is received by the at least one server from an automated transaction

machine in operative communication with the at least one server through a network. Claims 36 also recites that in (d) the automated transaction machine includes the display device. Nowhere do the applied references disclose or suggest this recited step.

The Action refers to paragraph [0114] of the Wheeler publication to support the rejection of claim 36. Paragraph [0114] of the Wheeler publication indicates that a device (250) communicates an electronic message that is digitally signed to an account authority (212). This teaching does not correspond to the steps recited in Appellants' claim 36.

For example, claim 36 is not directed to an automated transaction machine that sends a digitally signed message to a server. Rather, claim 36 recites that the at least one server receives a financial account number from the automated transaction machine which includes a display device through which the electronic document is displayed. Claim 36 also recites that the server is responsive to data representative of this financial account number received from the automated transaction machine, to cause a private key which corresponds to this data to be accessed from at least one data store in operative connection with the at least one server. Nowhere does the applied art disclose or suggest causing through operation of the at least one server, responsive to data associated with the financial account number received from an automated transaction machine, a private key which corresponds to the data to be accessed from at least one data store in operative connection with the at least one server. Further, nowhere does the applied art disclose or suggest displaying an electronic document through a display device of the automated transaction machine and causing through operation of the at least one server, a digital signature to be produced for this electronic document responsive to the private key.

The Office has not established *prima facie* obviousness with respect to claim 36, and it is respectfully submitted that the rejection should be reversed.

Claim 37

Claim 37 depends from claim 36 and recites that in (a) the automated transaction machine includes a cash dispenser. Nowhere do the applied references disclose or suggest this recited step.

As discussed previously with respect to claim 36, the Wheeler publication indicates that a device (250) communicates an electronic message that is digitally signed to an account authority (212). This teaching does not correspond to the steps recited in claim 37.

Nowhere does the applied art disclose or suggest causing through operation of the at least one server responsive to data associated with the financial account number received from an automated transaction machine including a cash dispenser, a private key which corresponds to the data to be accessed from at least one data store in operative connection with the at least one server. Further nowhere does the applied art disclose or suggest displaying an electronic document through a display device of the automated transaction machine including a cash dispenser, and causing through operation of the at least one server, a digital signature to be produced for this electronic document responsive to the private key.

The Office has not established *prima facie* obviousness with respect to claim 37, and it is respectfully submitted that the rejection should be reversed.

Claim 38

Claim 38 depends from claim 33 and recites that the method further comprises:

(e) receiving with the at least one server, the electronic document; and (f) causing through

operation of the at least one server the electronic document to be stored in the at least one data store in correlated relation with the data associated with the financial account received in (a).

Nowhere do the applied references disclose or suggest these recited steps.

The Action refers to paragraph [0170] of the Wheeler publication to support the rejection of claim 38. Paragraph [0170] of the Wheeler publication indicates that data fields in an electronic communication (7601) may be stored. However, where does the Wheeler publication disclose or suggest that such communications are stored in correlated relation with data associated with a financial account? The Action has failed to show where each and every feature recited in the claim is disclosed or suggested in the prior art.

Further, the description relied on in paragraph [0170] of the Wheeler publication to base the rejection does not qualify as prior art to Appellants' invention. The Action alleges (at page 4) that paragraph [0170] of the Wheeler publication is supported by pages 3-6 of the "Aadsstraw" portion of the Wheeler provisional. However, nowhere does this portion disclose or suggest that the described system stores an electronic document. Thus the asserted relevant portions of paragraph [0170] of the Wheeler publication are not supported by the Wheeler provisional, and therefore are not prior art.

Further, nowhere does the applied art disclose or suggest both: causing through operation of the at least one server a digital signature to be produced for an electronic document, responsive to the private key accessed responsive to data associated with a financial account; and causing through operation of the at least one server the electronic document to be stored in the at least one data store in correlated relation with the data associated with the financial account.

The portions relied on in the Wheeler publication as the basis for the rejection do not qualify as prior art. In addition, the Wheeler publication and Cohen do not disclose or suggest each of the features and relationships recited in the claim. Thus, the Office has not established *prima facie* obviousness. On this basis, it is respectfully submitted that the rejection of claim 38 should be reversed.

Claim 39

Claim 39 depends from claim 38 and recites that the method further comprises: (g) subsequent to (f) receiving with at least one server, data associated with the financial account from a remote computer in operative communication with the at least one server through a network. In addition claim 39 recites that the method comprises: (h) causing through operation of the at least one server the electronic document to be accessed from the at least one data store responsive to the data associated with the financial account received in (g). In addition, claim 39 recites that the method comprises: (i) causing through operation of the at least one server, the electronic document to be communicated to the remote computer. Nowhere do the applied references disclose or suggest these recited steps.

The Action alleges that Cohen teaches these recited features at page 12, lines 7-14. Appellants disagree. Page 12, lines 7-14, refer to an online electronic lockbox. Nowhere in this description of this online electronic lockbox, or anywhere else, does Cohen disclose or suggest causing through operation of the at least one server the electronic document to be accessed from at least one data store responsive to data associated with a financial account received from a

remote computer. The Wheeler publication also does not disclose or suggest these features recited in claim 39.

The Office has not established *prima facie* obviousness with respect to claim 39, and it is respectfully submitted that the rejection should be reversed.

Claim 41

Claim 41 recites computer readable media bearing instructions which are operative to cause at least one computer processor in the at least one server to cause the at least one server to carry out the method steps recited in claim 33.

The rejection of claim 41 should be reversed for at least the same reasons discussed with respect to claim 33. In addition, the Office has failed to show where the prior art discloses or suggests computer readable media bearing instructions which are operative to cause at least one computer processor in at least one server to cause the at least one server to carry out the method steps recited in claim 33. Thus the Office has not established *prima facie* obviousness with respect to claim 41. It is respectfully submitted that the rejection should be reversed on this basis, and for the reasons discussed with respect to claim 33.

Rejection under 35 U.S.C. § 103(a) over the Wheeler Publication in view of Cohen and Randle

In the Action, claims 7, 12-14, and 40 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the Wheeler publication in view of Cohen as applied to claims 1 and 11 and further in view of Randle. These rejections are respectfully traversed.

Claim 7

Claim 7 depends from claim 1 and recites that each digital safe deposit account is associated with at least one digital certificate. In addition, claim 7 recites that the computer processor is operative to cause the digital signature and at least one of the digital certificates associated with the one digital safe deposit account to be attached to the electronic document. Nowhere do the applied references disclose or suggest these recited features.

The Action admits that Wheeler and Cohen do not disclose or suggest the features recited in claim 7. However, the Action asserts that Randle teaches that customers can gain access to resources by using a certificate related to an account. Further, the Action asserts that it would be obvious based on an alleged motivation in Randle at column 11, lines 20-38 to modify the method disclosed in the Wheeler publication to cause a digital certificate to be generated and stored in association with the digital safe deposit account. Appellants disagree.

Column 11, lines 20-38, of Randle indicates that customer access to the bank may be Intranet or web-based or through kiosk terminals by way of an account certificate. Randle does not disclose or suggest that such an account certificate is stored in a digital safe deposit account. Further, nowhere does the Action show where Randle or any of the other applied references, disclose or suggest a computer processor that is operative to cause the digital signature and at least one of the digital certificates associated with the one digital safe deposit account to be attached to the electronic document.

The Office has not established *prima facie* obviousness with respect to claim 7, and it is respectfully submitted that the rejection should be reversed.

Claim 12

Claim 12 depends from claim 11 and recites that the computer processor is operative to cause a digital certificate to be generated and stored in association with the new digital safe deposit account, wherein the digital certificate includes the public key. Nowhere do the applied references disclose or suggest these recited features.

The Action admits that Wheeler and Cohen do not disclose or suggest the features recited in claim 12. However, the Action asserts that Randle teaches that customers can gain access to resources by using a certificate related to an account. Further, the Action asserts that it would be obvious based on an alleged motivation in Randle at column 11, lines 20-38, to modify the method disclosed in the Wheeler publication to cause a digital certificate to be generated and stored in association with the digital safe deposit account. Appellants disagree.

Column 11, lines 20-38, of Randle indicates that a customer's access to the bank may be Intranet or web-based or through kiosk terminals by way of an account certificate. Randle does not disclose or suggest that such an account certificate is stored in a digital safe deposit account.

The Office has not established *prima facie* obviousness with respect to claim 12, and it is respectfully submitted that the rejection should be reversed.

Claim 13

Claim 13 depends from claim 12 and recites that the computer processor is operative to receive a financial account number from the at least one ATM. In addition, claim 13 recites that the computer processor is operative to store the financial account number in association with the

new digital safe deposit account. Nowhere do the applied references disclose or suggest these recited features.

The Action refers to paragraphs [0184] - [0185] of the Wheeler publication to support the rejection of claim 13. These paragraphs of the Wheeler publication indicate that each account includes a unique account identifier comprising an account number (716). However, nowhere does the Wheeler publication nor any of the other applied references, disclose or suggest that a computer processor is operative to store a financial account number or any other account number received from an ATM, in a digital safe deposit account.

The Office has not established *prima facie* obviousness with respect to claim 13, and it is respectfully submitted that the rejection should be reversed.

Claim 14

Claim 14 depends from claim 13 and recites that the computer processor is operative to receive a password input from the at least one ATM. In addition, claim 14 recites that the computer processor is operative to store the password input in association with the new digital safe deposit account. Nowhere do the applied references disclose or suggest these recited features.

The Action refers to paragraph [0187] of the Wheeler publication to support the rejection of claim 14. This paragraph of the Wheeler publication indicates that an ATM may receive input of a PIN. Although a PIN may correspond to a password, nowhere does the Wheeler publication nor any of the other applied references, disclose or suggest that a computer processor is operative to store a password (or a PIN) received from an ATM, in a digital safe deposit account.

The Office has not established *prima facie* obviousness with respect to claim 14, and it is respectfully submitted that the rejection should be reversed.

Claim 40

Claim 40 depends from claim 33 and recites that the method further comprises: (e) causing through operation of the at least one server at least one digital certificate associated with the private key to be accessed from the at least one data store. The at least one digital certificate was previously stored in the at least one data store in correlated relation with the data associated with the financial account. In addition, claim 40 recites that the method comprises: (f) causing through operation of the at least one server, the at least one digital certificate to be attached to the electronic document during or after the display of the electronic document through the display device. Nowhere do the applied references disclose or suggest these recited steps.

The Action admits that Wheeler and Cohen do not disclose or suggest the steps recited in claim 40. However, the Action asserts that Randle teaches that customers can gain access to resources by using a certificate related to an account. Further, the Action asserts that it would be obvious based on an alleged motivation in Randle at column 11, lines 20-38, to modify the method disclosed in the Wheeler publication to access the digital certificate that was previously stored in association with the account, as well as to display the document with the attached digital certificate. Appellants disagree.

Column 11, lines 20-38, of Randle indicates that customer access to the bank may be Intranet or web-based or through kiosk terminals by way of an account certificate. Where does Randle disclose or suggest that such an account certificate is stored in a data store in correlated

relation with data associated with a financial account? Further, where does Randle disclose or suggest a server that attaches the account certificate to an electronic document during or after the display of the electronic document?

The Office has not established *prima facie* obviousness with respect to claim 40. It is respectfully submitted that the rejection should be reversed on this basis.

**Rejection under 35 U.S.C. § 103(a) over the Wheeler Publication in view of
Cohen and Meurer**

In the Action, claims 17 and 18 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the Wheeler publication in view of Cohen as applied to claim 1 and further in view of Meurer. These rejections are respectfully traversed.

Claim 17

Claim 17 depends from claim 1 and recites that the computer processor is operative to cause a digital signature processing fee to be assessed to a financial account in response to causing the digital signature to be produced for the electronic document. Nowhere do the applied references disclose or suggest these recited features.

The Action admits that Wheeler and Cohen do not disclose or suggest the features recited in claim 17. However, the Action asserts that Meurer teaches assessing a processing fee collected for processing transactions. Further, the Action asserts that it would be obvious, based on an alleged motivation in Meurer at paragraph [0013], to modify the method disclosed in the Wheeler publication to cause a digital signature processing fee to be accessed to a financial

account in response to producing the digital signature for the electronic document. Appellants disagree.

Although paragraph [0013] of Meurer indicates that surcharge and interchange fees may be charged for dispensing cash from an ATM, nowhere does Meurer disclose or suggest assessing a digital signature processing fee. Nowhere does Meurer disclose or suggest charging fees for the production of digital signatures for electronic document. Thus the applied references do not disclose or suggest a computer processor that is operative to cause a digital signature processing fee to be assessed to a financial account in response to causing the digital signature to be produced for the electronic document.

The Office has not established *prima facie* obviousness with respect to claim 17. In addition, there is no prior art teaching, suggestion, or motivation cited for modifying the Wheeler publication and Cohen in view of Meurer so as to produce the claimed invention.

On this basis, it is respectfully submitted that the rejection of claim 17 should be reversed.

Claim 18

Claim 18 depends from claim 17 and recites that the computer processor is operative to receive information about the financial account from the at least one ATM. Nowhere do the applied references disclose or suggest these recited features.

The Action refers to paragraph [0190] of the Wheeler publication to support the rejection of claim 18. This paragraph of the Wheeler publication indicates that the ATM (660) transmits a message to a financial institution (612). Although Wheeler indicates that the message transmitted from the ATM may include an account number, nowhere does Wheeler disclose or suggest that the account number sent in the message from the ATM is ever used to assess a

digital signature processing fee. Thus the applied references do not disclose or suggest a computer processor that is operative to cause a digital signature processing fee to be assessed to a financial account, about which information is received from an ATM.

The Office has not established *prima facie* obviousness with respect to claim 18, and it is respectfully submitted that the rejection should be reversed.

Rejection under 35 U.S.C. § 103(a) over the Wheeler Publication in view of Cohen

In the Action, claims 20-21, 23, 25-26, and 31-32 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the Wheeler publication. These rejections are respectfully traversed.

Claim 20

Claim 20 is an independent claim which is directed to a method. The method comprises: (a) receiving a financial account number from an automated transaction machine; (b) accessing a private key associated with the financial account number; and (c) enabling an electronic document displayed by the automated transaction machine to be digitally signed with the private key.

The Wheeler provisional does not support the portions in the Wheeler publication relied on by the Action to reject claim 20. Thus the portions of the Wheeler publication relied on to reject claim 20 are not entitled to prior art status with respect to claim 20.

For example, the Action supported the rejection of claim 20 based on paragraph [0190] of the Wheeler publication. Paragraph [0190] of the Wheeler publication discusses that a message generated by an ATM is transmitted to a card (650) for digitally signing by a card using a private

key stored in the card. The Action alleges (at page 5) that paragraph [0190] of the Wheeler publication is supported by pages 1-2 of the "Aadsbrnd" portion of the Wheeler provisional. However, nowhere do these portions of the Wheeler provisional disclose an electronic message which is transmitted to a card by an ATM for digitally signing by the card using a private key retained in the card. Thus the asserted relevant portions of paragraph [0190] of the Wheeler publication are not supported by the Wheeler provisional, and therefore are not prior art with respect to claim 20. The Office has not established *prima facie* obviousness, and the rejection of claim 20 should be reversed.

In addition, even if it were somehow possible for the Wheeler provisional to support the Wheeler publication, the Wheeler publication still does not disclose or suggest all of the features and relationships recited in claim 20. For example, nowhere do the applied references disclose or suggest:

- accessing a private key associated with the financial account number; and
- enabling an electronic document displayed by the automated transaction machine to be digitally signed with the private key.

Although, the Action does not state which elements of Wheeler correspond to respective elements recited in claim 20, it appears that the Office may regard the card discussed in paragraph [0190] as corresponding to the element which carries out steps (b) through (c) of claim 20. However, Appellants respectfully submit that nowhere does Wheeler disclose or suggest that these steps are carried out by the described card or by any other device described in the Wheeler publication.

For example, with respect to step (b), nowhere does the Wheeler publication disclose or suggest accessing a private key associated with a financial account number received from an automated transaction machine. Although paragraph [0189] indicates that the message transmitted by the ATM may include an account number therein, nowhere does the Wheeler publication disclose or suggest that the card (650) accesses the private key retained therein responsive to the account number.

The Action asserts that the Wheeler publication at paragraph [0113] teaches that an account number is needed in order to utilize the public/private key pair. However, paragraph [0113] does not state this. Rather, this portion of the Wheeler publication indicates that the account authority (212) maintains an association between the account and the public key (218). Although the account number could be used to access the public key, nowhere does the Wheeler publication disclose or suggest that the card or any other device requires an account number to access the private key stored in the card or other device. In addition as discussed previously with respect to claim 1, the Wheeler provisional does not support paragraph [0113] of the Wheeler publication.

Further, with respect to step (c), nowhere does the Wheeler publication disclose or suggest enabling an electronic document displayed by the automated transaction machine to be digitally signed with the private key. In paragraph [0189] the Wheeler publication indicates that the ATM (660) displays a menu of operations which include money withdrawal, balance inquiry, statement request, money transfer, money deposit, bill payment. However such a menu displayed by an ATM does not disclose or inherently require a message to be displayed by the ATM which has been or will be digitally signed with a private key. In addition, the message from the ATM

that is signed by a card in the Wheeler publication (paragraph [0190]) corresponds to an instruction to the financial institution corresponding to the desired operation of the account holder (paragraph [0189]). Nowhere does the Wheeler publication disclose or suggest that such a message is ever displayed by the ATM. Nor would displaying such a message be inherent in the Wheeler publication, as such a message could be transferred from the ATM to a financial institution without an need for a user to view it on a display of the ATM.

Anticipation by inherency requires that the Patent Office establish that persons skilled in the art would recognize that the missing element is necessarily present in the reference. To establish inherency the Office must prove through citation to prior art that the feature alleged to be inherent is "necessarily present" in a cited reference. Inherency may not be established based on probabilities or possibilities. It is plainly improper to reject a claim on the basis of 35 U.S.C. § 102 based merely on the possibility that a particular prior art disclosure could or might be used or operated in the manner recited in the claim. *In re Robertson*, 169 F.3d 743, 49 U.S.P.Q.2d 1949 (Fed. Cir. 1999).

Nowhere does the applied art explicitly or inherently disclose or suggest enabling an electronic document displayed by the automated transaction machine to be digitally signed with the private key.

As discussed previously, the portions relied on in Wheeler publication to base the rejection of claim 20, do not qualify as prior art. In addition, even if the Wheeler publication qualified as prior art (which it does not), Appellants respectfully submit that the Office has not *established prima facie* obviousness with respect to claim 20. The Wheeler publication does not disclose or suggest each and every element, feature, relationship and step of the claimed

invention arranged in the manner recited in the claim, as is required to sustain the rejection. Nor is there any prior art teaching, suggestion, or motivation cited for modifying the Wheeler publication so as to produce the claimed invention. Further, it would not have been obvious to one having ordinary skill in the art to have modified the Wheeler publication to have produced the claimed invention. Appellants respectfully submit that the 35 U.S.C. § 103(a) rejection of claim 20 is improper and should be reversed. It follows that the rejections of claims 21-26 which depend from claim 20 should also be reversed.

Claim 21

Claim 21 depends from claim 20 and recites that prior to step (c) the method further comprises: (d) receiving a password from the automated transaction machine, and (e) verifying that the password corresponds to a valid password previously associated with the financial account number. Nowhere does the applied art disclose or suggest these recited steps.

Nowhere does the Wheeler publication disclose or suggest receiving and verifying a password received from an automated transaction machine prior to enabling an electronic document displayed by the automated transaction machine to be digitally signed with the private key.

The Office has not established *prima facie* obviousness with respect to claim 21, and it is respectfully submitted that the rejection should be reversed.

Claim 23

Claim 23 depends from claim 20 and recites that the method further comprises: (d) storing a digitally signed copy of the electronic document in a digital safe deposit account in

association with the financial account number. Nowhere does the applied art disclose or suggest this recited step.

The Action refers to paragraph [0170] of the Wheeler publication to support the rejection of claim 23. Paragraph [0170] of the Wheeler publication indicates that data fields in an electronic communication (7601) may be stored. However, where does the Wheeler publication disclose or suggest that such communications are stored in association with a digital safe deposit account as recited, or in association with any other type of account? The Action has failed to show where each and every feature recited in the claim is disclosed or suggested in the prior art.

Further, the description relied on in paragraph [0170] of the Wheeler publication which is relied on by the Action as the basis for the rejection, does not qualify as prior art. The Action alleges (at page 4) that paragraph [0170] of the Wheeler publication is supported by pages 3-6 of the "Aadsstraw" portion of the Wheeler provisional. However, nowhere does this portion disclose or suggest that the described system stores an electronic document. Thus the asserted relevant portions in paragraph [0170] of the Wheeler publication are not supported by the Wheeler provisional, and therefore are not prior art.

Further, nowhere does the applied art disclose or suggest a method that stores an electronic document that was displayed by an automated transaction machine. Also, nowhere does the applied art disclose or suggest storing an electronic document displayed by an automated transaction machine, in a data store in association with an account. Further, nowhere does the applied art disclose or suggest storing an electronic document displayed by an automated transaction machine, in a digital safe deposit account. In addition nowhere does the applied art disclose or suggest storing an electronic document displayed by an automated

transaction machine, in a digital safe deposit account in association with a financial account number.

The portions relied on in the Wheeler publication as the basis for the rejection do not qualify as prior art. In addition, the Wheeler publication does not disclose or suggest each of the features, relationships, and steps recited in the claim. Thus the Office has not established *prima facie* obviousness. For these reasons it is respectfully submitted that the rejection of claim 23 should be reversed.

Claim 25

Claim 25 depends from claim 20 and recites that the method further comprises: (d) enabling the electronic document to be digitally time stamped. Nowhere does the applied art disclose or suggest this recited step.

The Action alleges that this feature is disclosed in the Wheeler publication at paragraph [0172]. However, the description relied on in paragraphs [0172] of the Wheeler publication to base the rejection, does not qualify as prior art. The Action alleges (at page 4) that paragraph [0172] of the Wheeler publication is supported by page 6 of the "Aadsstraw" portion of the Wheeler provisional. However, this portion only states that a unique message includes a "data/time". Nowhere does the Wheeler provisional disclose or suggest enabling the electronic document to be digitally time stamped. Thus the portion of the Wheeler publication used as a basis to reject the claim, does not qualify as prior art.

The Office has not established *prima facie* obviousness with respect to claim 25, and it is respectfully submitted that the rejection should be reversed.

Claim 26

Claim 26 depends from claim 20 and recites that the method further comprises: (d) dispensing cash from the automated transaction machine. Nowhere does the applied art disclose or suggest this recited step.

Nowhere does the Wheeler publication disclose or suggest both dispensing cash from an automated transaction and enabling an electronic document displayed by the same automated transaction machine to be digitally signed.

The Office has not established *prima facie* obviousness with respect to claim 26, and it is respectfully submitted that the rejection should be reversed.

Claim 31

Claim 31 is an independent claim which is directed to a method. The method comprises: (a) receiving a request at an ATM to digitally sign an electronic document visually displayed by the ATM; (b) causing a digital signature and a digital time stamp to be produced for the electronic document; and (c) causing the digital signature and the digital time stamp to be attached to the electronic document.

The Wheeler provisional does not support the portions relied on in the Wheeler publication to reject the claim 31. Thus the portions of the Wheeler publication relied on to reject claim 31 are not entitled to prior art status with respect to claim 31.

For example, the Action supported the rejection of claim 31 based on paragraph [0115] of the Wheeler publication. Paragraph [0115] of the Wheeler publication discusses that a message can include a "date and time stamp". The Action alleges (at page 3) that paragraph [0115] of the

Wheeler publication is supported by pages 12-13 of the "Aadsstraw" portion and page 3 of the "Aadsbrnd" portion of the Wheeler provisional. However, nowhere do these portions of the Wheeler provisional disclose or suggest that a message includes a date and time stamp.

In addition, as discussed with respect to claims 19 and 25, page 6 of the "Aadsstraw" portion of the Wheeler provisional also does not support the "digital time stamp" discussed at paragraph [0172] of the Wheeler publication. For example, page 6 of the "Aadsstraw" portion of the Wheeler provisional only states that a unique message includes a "data/time". Nowhere does the Wheeler provisional disclose or suggest causing a "digital time stamp" to be produced and attached to an electronic document. Thus the Wheeler publication is not supported by the Wheeler provisional, and is not prior art with respect to Appellants' recited features.

In addition, claim 31 recites causing both a digital signature and a digital time stamp to be produced for the electronic document and to be attached to the electronic document. Nowhere does the Wheeler provisional disclose or suggest producing a digital signature and a digital time stamp for an electronic document, and attaching the digital signature and the digital time stamp to the electronic document.

Thus the allegedly relevant portions of paragraph [0115] or [0172] of the Wheeler publication, are not supported by the Wheeler provisional and therefore are not prior art with respect to claim 31. The Office has not established *prima facie* obviousness and the rejection of claim 31 should be reversed.

In addition, the Action admits that the Wheeler publication does not disclose step (a) of claim 31. However, the Action asserts that in another embodiment, the ATM has a display window so that customers can choose from the possible operations. The Action then asserts

based on the alleged teaching by the Wheeler publication at paragraphs [188] - [189] that it would have been obvious to modify the method disclosed in the Wheeler publication to visually display a message to be signed, which includes the operation chosen. Appellants disagree.

In paragraph [0189] the Wheeler publication indicates that the ATM (660) displays a menu of operations which include money withdrawal, balance inquiry, statement request, money transfer, money deposit, bill payment. However, such a menu displayed by an ATM does not disclose or inherently require a message to be displayed by the ATM, which has been or will be digitally signed with a private key. In addition, the message from the ATM that is signed by a card in the Wheeler publication (paragraph [0190]), corresponds to an instruction to the financial institution corresponding to the desired operation of the account holder (paragraph [0189]). Nowhere does the Wheeler publication disclose or suggest that such a message is ever displayed by the ATM. Nor would displaying such a message be inherent in the Wheeler publication, as such a message could be transferred from the ATM to a financial institution responsive to a menu selection without an need for a user to view the message on the ATM.

Anticipation by inherency requires that the Patent Office establish that persons skilled in the art would recognize that the missing element is necessarily present in the reference. To establish inherency the Office must prove through citation to prior art that the feature alleged to be inherent is "necessarily present" in a cited reference. Inherency may not be established based on probabilities or possibilities. It is plainly improper to reject a claim on the basis of 35 U.S.C. § 102 based merely on the possibility that a particular prior art disclosure could or might be used or operated in the manner recited in the claim. *In re Robertson*, 169 F.3d 743, 49 U.S.P.Q.2d 1949 (Fed. Cir. 1999).

Nowhere does the applied art explicitly or inherently disclose or suggest receiving a request at an ATM to digitally sign an electronic document visually displayed by the ATM.

As discussed previously, the portions relied on in Wheeler publication to base the rejection of claim 31, do not qualify as prior art. In addition, even if the Wheeler publication qualified as prior art (which it does not), Appellants respectfully submit that the Office has not *established prima facie* obviousness with respect to claim 31. The Wheeler publication does not disclose or suggest each and every element, feature, relationship and step of the claimed invention arranged in the manner recited in the claim, as is required to sustain the rejection. Nor is there any prior art teaching, suggestion, or motivation cited for modifying the Wheeler publication so as to produce the claimed invention. Further, it would not have been obvious to one having ordinary skill in the art to have modified the Wheeler publication to have produced the claimed invention. Appellants respectfully submit that the 35 U.S.C. § 103(a) rejection of claim 31 is improper and should be reversed. It follows that the rejection of claim 32 which depend from claim 31 should also be reversed.

Claim 32

Claim 32 depends from claim 31 and recites that the method further comprises: (d) dispensing cash from the ATM. Nowhere does the applied art disclose or suggest this recited step.

Nowhere does the Wheeler publication disclose or suggest both dispensing cash from an ATM and receiving a request at the same ATM to digitally sign an electronic document visually displayed by the ATM.

The Office has not established *prima facie* obviousness with respect to claim 32, and it is respectfully submitted that the rejection should be reversed.

Rejection under 35 U.S.C. § 103(a) over the Wheeler Publication in view of Cohen and Randle

In the Action, claim 22 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Wheeler in view of Cohen as applied to claim 20 and further in view of Randle. This rejection is respectfully traversed.

Claim 22

Claim 22 depends from claim 20 and recites that the method further comprises: (d) accessing a digital certificate previously associated with the financial account number. The digital certificate includes a public key that corresponds to the private key. The public key is capable of being used to validate the digital signature. In addition claim 22 recites that the method comprises: (e) enabling the digital certificate to be associated with the electronic document. Nowhere do the applied references disclose or suggest these recited steps.

The Action admits that Wheeler does not disclose or suggest the steps recited in claim 22. However, the Action asserts that Randle teaches that customers can gain access to resources by using a certificate related to an account. Further, the Action asserts that it would be obvious based on an alleged motivation in Randle at column 11, lines 20-38, to modify the method disclosed in the Wheeler publication to access the digital certificate associated with the account in order to authenticate the entity's digital signature and to further associate the electronic document with the certificate. Appellants disagree.

Column 11, lines 20-38, of Randle indicates that a customer's access to the bank may be Intranet or web-based or through kiosk terminals by way of an account certificate. However, where does Randle disclose or suggest that such an account certificate is associated with a financial account number? It does not.

The Office has not established *prima facie* obviousness with respect to claim 22. It is respectfully submitted that the rejection should be reversed on this basis.

**Rejection under 35 U.S.C. § 103(a) over the Wheeler Publication in view of
Cohen and Meurer**

In the Action, claim 24 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Wheeler in view of Cohen as applied to claim 20 and further in view of Meurer. This rejection is respectfully traversed.

Claim 24

Claim 24 depends from claim 20 and recites that the method further comprises: (d) receiving a second financial account number from the automated transaction machine; and e) assessing a processing fee associated with the digital signing of the electronic document to a financial account associated with the second financial account number. Nowhere do the applied references disclose or suggest these recited steps.

The Action admits that Wheeler does not disclose or suggest step (e) of claim 24. However, the Action asserts that Meurer teaches assessing a processing fee collected for processing transactions. Further the Action asserts that it would be obvious based on an alleged

motivation in Meurer at paragraph [0013], to modify the method disclosed in the Wheeler publication to cause a digital signature processing fee to be accessed to a financial account in response to producing the digital signature for the electronic document. Appellants disagree.

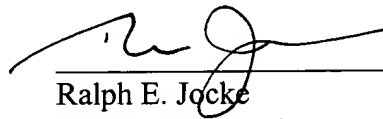
Although paragraph [0013] of Meurer indicates that surcharge and interchange fees may be charged for dispensing cash from an ATM, nowhere does Meurer disclose or suggest charging fees for the digital signing of an electronic document. Thus the applied references do not disclose or suggest receiving a second financial account number from the automated transaction machine and assessing a processing fee associated with the digital signing of the electronic document to a financial account associated with the second financial account number.

The Office has not established *prima facie* obviousness with respect to claim 24. In addition, there is no prior art teaching, suggestion, or motivation cited for modifying the Wheeler publication in view of the Meurer so as to produce the claimed invention. On this basis, it is respectfully submitted that the rejection of claim 17 should be reversed.

CONCLUSION

Each of Appellants' pending claims specifically recites elements, relationships, and steps that are neither disclosed nor suggested in any of the applied prior art. Furthermore, the applied prior art is devoid of any teaching, suggestion, or motivation for producing the recited invention. For these reasons it is respectfully submitted that all the pending claims are allowable.

Respectfully submitted,



Ralph E. Jocke
WALKER & JOCKE
231 South Broadway
Medina, Ohio 44256
(330) 721-0000

Reg. No. 31,029



(viii)

CLAIMS APPENDIX

1. An apparatus comprising:

at least one computer processor; and

at least one data store in operative connection with the computer processor, wherein the at least one data store includes a plurality of digital safe deposit accounts stored therein, wherein each of the digital safe deposit accounts is associated with at least one private key, wherein the computer processor is operative to communicate with a plurality of ATMs, wherein the computer processor is operative responsive to at least one of the ATMs to cause a digital signature to be produced for an electronic document responsive to the private key associated with one of the digital safe deposit accounts.

2. The apparatus according to claim 1 wherein the computer processor is operative to receive the electronic document from the at least one ATM, wherein the computer processor is operative to store the electronic document in the data store in association with the one digital safe deposit account.

3. The apparatus according to claim 2 wherein the computer processor is operative to retrieve the electronic document from the data store and send the electronic document to any one of the plurality of ATMs.

4. The apparatus according to claim 2 wherein the computer processor is operative to encrypt and decrypt the electronic document stored in the at least one data store responsive to a secret key received from the at least one ATM.

5. The apparatus according to claim 1 wherein each digital safe deposit account is associated with a financial account number, wherein the computer processor is operative to access the private key associated with the one digital safe deposit account responsive to a message received from the at least one ATM which includes a financial account number that corresponds to the financial account number associated with the one digital safe deposit account.

6. The apparatus according to claim 5, wherein the at least one financial account number corresponds to a credit card number.

7. The apparatus according to claim 1 wherein each digital safe deposit account is associated with at least one digital certificate, wherein the computer processor is operative to cause the digital signature and at least one of the digital certificates associated with the one digital safe deposit account to be attached to the electronic document.

8. The apparatus according to claim 1 wherein the computer processor is operative to maintain and store in the at least one data store, an access log in association with each digital safe deposit account.

9. The apparatus according to claim 1 wherein the at least one ATM includes a cash dispenser, wherein the computer processor is operative through communication with a financial transaction processing system to cause a dispense of cash from the cash dispenser to be authorized.

10. The apparatus according to claim 1 wherein the computer processor is operative to cause a new digital safe deposit account to be created in the data store responsive to communication from the at least one ATM.

11. The apparatus according to claim 10 wherein the computer processor is operative to cause a new private key and a corresponding public key to be produced responsive to communication from the at least one ATM, wherein the computer processor is operative to store the private key in association with the new digital safe deposit account.

12. The apparatus according to claim 11 wherein the computer processor is operative to cause a digital certificate to be generated and stored in association with the new digital safe deposit account, wherein the digital certificate includes the public key.

13. The apparatus according to claim 12 wherein the computer processor is operative to receive a financial account number from the at least one ATM, wherein the computer processor is operative to store the financial account number in association with the new digital safe deposit account.

14. The apparatus according to claim 13 wherein the computer processor is operative to receive a password input from the at least one ATM, wherein the computer processor is operative to store the password input in association with the new digital safe deposit account.

15. The apparatus according to claim 1 wherein the computer processor is operative to receive a one-way hash of the electronic document from the at least one ATM, wherein the computer processor is operative to cause the digital signature to be generated responsive to the one-way hash and the private key.

16. The apparatus according to claim 1 wherein the computer processor is operative to cause a second digital signature to be produced for the electronic document responsive to a private key that is not associated with the one digital safe deposit account.

17. The apparatus according to claim 1 wherein the computer processor is operative to cause a digital signature processing fee to be assessed to a financial account in response to causing the digital signature to be produced for the electronic document.

18. The apparatus according to claim 17 wherein the computer processor is operative to receive information about the financial account from the at least one ATM.

19. The apparatus according to claim 1 wherein the computer processor is operative to cause a digital time stamp to be produced and attached to the electronic document.

20. A method comprising:

- a) receiving a financial account number from an automated transaction machine;
- b) accessing a private key associated with the financial account number; and
- c) enabling an electronic document displayed by the automated transaction machine to be digitally signed with the private key.

21. The method according to claim 20, wherein prior to step (c) further comprising:

- d) receiving a password from the automated transaction machine; and
- e) verifying that the password corresponds to a valid password previously associated with the financial account number.

22. The method according to claim 20, further comprising:

- d) accessing a digital certificate previously associated with the financial account number, wherein the digital certificate includes a public key that corresponds to the private key, wherein the public key is capable of being used to validate the digital signature; and
- e) enabling the digital certificate to be associated with the electronic document.

23. The method according to claim 20, further comprising:

- d) storing a digitally signed copy of the electronic document in a digital safe deposit account in association with the financial account number.

24. The method according to claim 20, further comprising:

- d) receiving a second financial account number from the automated transaction machine; and
- e) assessing a processing fee associated with the digital signing of the electronic document to a financial account associated with the second financial account number.

25. The method according to claim 20, further comprising:

- d) enabling the electronic document to be digitally time stamped.

26. The method according to claim 20, further comprising:

- d) dispensing cash from the automated transaction machine.

27. A method comprising:

- a) receiving a request from an automated transaction machine to digitally sign an electronic document visually displayed by the automated transaction machine, wherein the request includes an account number that is associated with a digital safe deposit account;
- b) accessing a private key associated with the digital safe deposit account responsive to the account number;
- c) producing a digital signature for the electronic document responsive to the private key; and
- d) causing the digital signature to be attached to the electronic document.

28. The method according to claim 27, further comprising:

- e) storing a digitally signed copy of the electronic document in a data store in association with the digital safe deposit account.

29. The method according to claim 27, wherein in step (a) the account number corresponds to a financial account number.

30. The method according to claim 27 and further comprising:

- e) dispensing cash from the automated transaction machine.

31. A method comprising:

- a) receiving a request at an ATM to digitally sign an electronic document visually displayed by the ATM;
- b) causing a digital signature and a digital time stamp to be produced for the electronic document; and

- c) causing the digital signature and the digital time stamp to be attached to the electronic document.

32. The method according to claim 31 and further comprising:

- d) dispensing cash from the ATM.

33. A method comprising:

- a) receiving with at least one server, data associated with a financial account;
- b) responsive to the data associated with the financial account received in (a), causing through operation of the at least one server, a private key which corresponds to the data associated with the financial account received in (a) to be accessed from at least one data store in operative connection with the at least one server, wherein the private key was previously stored in the at least one data store in correlated relation with the data associated with the financial account;
- c) causing through operation of the at least one server, a digital signature to be produced for an electronic document responsive to the private key accessed in (b);
and

- d) causing through operation of the at least one server, the digital signature to be attached to the electronic document during or after the display of the electronic document through a display device viewable by a customer associated with the financial account.

34. The method according to claim 33, wherein in (a) the data associated with the financial account is representative of a financial account number.

35. The method according to claim 34, wherein in (a) the at least one financial account number corresponds to at least one of a credit card number, a debit card number, and a bank account number.

36. The method according to claim 34, wherein in (a) the data representative of the financial account number is received by the at least one server from an automated transaction machine in operative communication with the at least one server through a network, wherein in (d) the automated transaction machine includes the display device.

37. The method according to claim 36, wherein in (a) the automated transaction machine includes a cash dispenser.

38. The method according to claim 33 and further comprising:

- e) receiving with the at least one server, the electronic document;
- f) causing through operation of the at least one server the electronic document to be stored in the at least one data store in correlated relation with the data associated with the financial account received in (a).

39. The method according to claim 38 and further comprising:

- g) subsequent to (f) receiving with at least one server, data associated with the financial account from a remote computer in operative communication with the at least one server through a network;
- h) causing through operation of the at least one server the electronic document to be accessed from the at least one data store responsive to the data associated with the financial account received in (g);
- I) causing through operation of the at least one server, the electronic document to be communicated to the remote computer.

40. The method according to claim 33 and further comprising:

- e) causing through operation of the at least one server at least one digital certificate associated with the private key to be accessed from the at least one data store, wherein the at least one digital certificate was previously stored in the at least one data store in correlated relation with the data associated with the financial account; and
- f) causing through operation of the at least one server, the at least one digital certificate to be attached to the electronic document during or after the display of the electronic document through the display device.

41. Computer readable media bearing instructions which are operative to cause at least one computer processor in the at least one server to cause the at least one server to carry out the method steps recited in claim 33.

(ix)

EVIDENCE APPENDIX

None.

(x)

RELATED PROCEEDINGS APPENDIX

No decisions have been rendered by a court or the Board with respect to U.S. application serial no. 09/683,944 filed March 5, 2002.



COURTESY COPY

U.S. Provisional Application No. 60/223,076 (Wheeler Provisional)

ATTACHMENT 1

INDEX TO ATTACHED PROVISIONAL APPLICATION SPECIFICATION "SYSTEMS AND METHODS FOR TRUSTED ELECTRONIC MESSAGES"

Attorney Docket: 4526-29628

Exhibit No.	Document Title	No. of Pages
1	Aads	7
2	Aadsstraw AADS Chip Infrastructures	14
3	Aadsbrnd AADS Brand Conventions	6
4	Rachip AADS Chip Strawman	8

004030-3402205

Aads

Some misc. issues facets looking at the issue around CADS and AADS infrastructures

infrastructure
payload and certificate compression
payload and X9.59
service operation

* infrastructure

AADS is straight-forward upgrade to all existing shared-secret authentication business processes (upgrade from shared secret to digital signature using existing business processes).

The CADS infrastructure grew up out of requirement for some sort of authentication processes for offline email which lacked not only an authentication infrastructure ... but any infrastructure what so ever (other than simple address to routing). Part of the problem with working on the Internet infrastructure from mid-80s until now was the lack of any origination verification. When I was putting together a payment gateway for the Internet in the '95 timeframe, as well as shooting a resource exhaustion problem in summer of '95 for one of the largest online service providers (nearly a year to the day when it hit the press in '96 for a similar type of problem) was the lack of anything to do with origination. Even when the Internet made the transition from fully-meshed routing to hierarchical routing .. there was no serious consideration of the ISPs verifying that the from IP-address on incoming packets corresponded to the subnet that they were suppose to originate from (similar to boundary packet filters checking to see that incoming packets from the internet don't have spoof'ed from IP-address of internal subnets).

For some references see:

The CADS certificates provide two useful functions:

1) free-standing authentication infrastructures for operations that

Aads

don't have any infrastructure of their own (typical of most offline email implementations)

2) free-standing technology demonstration platforms.

Rather than starting with the premise that CADS is the answer and searching for the question, it has been useful to look at existing financial industry authentication business processes and look at what

aspects of technology that is in use by CADS platforms that could be easily and directly applied. Almost all financial industry authentication transactions are integrated with business transaction that reference an account record as part of executing the transaction

(i.e. authentication isn't being performed solely for the sake of doing authentication but as part of some business operation). The existing deployed authentication technology is primarily based on some

form of shared secret (PIN number, mother's maiden name, social security number, birth date, address, etc, although many of these shared secrets are not so secret).

Public key technology provides an opportunity for directly and easily

upgrading all the existing authentication transactions to a more secure level. Public key technology has the immediate obvious advantage that the value used for authenticating a transaction is not

the same as the value used for originating a transaction. Recording a

public key in place of an account record secret key has the advantage

that people that view the account record, no longer can originate fraudulent transactions just by knowing the recorded value.

This potentially has consumer ease of use implications. Current use of identical shared secrets across different domains is inhibited because

of the lack of cross-domain liability i.e. protections are in place for mis-use of a shared secret within a specific business domain, but

there is less protection when a shared secret learned in one domain is

then fraudulently used in another domain. There are situations of people actually listing different "mother's maiden name" in every domain that they register. Public key registration has the advantage

Aads

that just knowing the public key does not allow fraudulent transactions to be originated.

In that sense, every existing non-face-to-face, authenticated transaction (electronic, ATM, credit, debit, telephone call center) could be upgraded to a higher integrity level by converting from shared secret paradigm to a public key paradigm. AADS describes a methodology for this simple and straight forward integrity upgrade while maintaining the existing business processes.

The business justification for an AADS upgrade to an existing authentication business process is an inexpensive integrated business solution with stronger integrity and lower risk.

* payload and certificate compression

Fundamentally a certificate binds various attributes to a public key for authentication purposes. As noted, this provides (nearly) a free-standing authentication environment for processes that don't currently don't have their own authentication business processes.

For eons, businesses have used account records to bind attributes, including the binding of authentication information (typically shared secrets).

Sometime in the '96(?) timeframe there was an IETF PKIX thread that looked at certificate compression, including data compression, information compression and knowledge compression methodologies. The objective was to satisfy both transmission overhead (redundant transmission of identical certificate information appended to every transaction) as well as the storage of a certificate copy in an account record at the registration authority (regardless of whether it was a CADS or AADS registration authority).

The highest level of transmission compression came on transactions with a central authority. This has since been typified by the financial institutions in the European Union meeting privacy mandates and other business requirements with "relying-party" only environment.

Aads

If all transactions are being sent to a party for which there already exists a business relationship and where a corresponding account record exists, then the highest level of compression is achieved by just using the account number (since all other information has already been registered in the account record). Resending any additional information (other than the account number) is a redundant and superfluous transmission of information that has already been registered in the account record.

Furthermore, for financial infrastructures, the base transaction will already contain the account number ... therefore appending it after the digital signature (in addition to having it in the body of the transaction) is also redundant and superfluous.

So:

- 1) sending more than the account number is redundant and superfluous for account-based transaction
- 2) sending the account number twice in a message is also redundant and superfluous
- 3) appending anything after the digital signature to an account-based transaction is redundant and superfluous

* payload and X9.59

The opportunity can also be looked at from another aspect. For all consumer account-based payment transactions that X9.59 covers, the existing legacy infrastructures measure payloads in terms of bytes and tens of bytes. The information-based template methodology for certificate compression is attempting to reduce certificate payloads from thousands of bytes to hundreds of bytes.

One of the X9.59 mappings has shown a knowledge-based compression

Aads

methodology that meets the business requirements of the existing financial infrastructures and provides end-to-end digital signature authentication. This recognizes that once the information is registered in the account record, it is redundant and superfluous to transmit it again (in this case, the certificate knowledge-based compression reduces the size of the transmitted certificate on every transaction to zero bytes ... not hundreds of bytes).

Note that while it is possible to do a AADS mapping for X9.59 consumer financial account-based payments, consumer account-based payments are not the only kind of financial transactions that currently have authentication infrastructures that would benefit from an AADS upgrade methodology.

* service operation

One of the interesting things is how various CADS-based technology demos back into an AADS-like infrastructure.

There have been some certificate-based technology demonstrations for consumer payments. They've had the characteristic that

- 1) stripped off digital signature at Internet boundary
- 2) did not provide for end-to-end digital signature authentication
- 3) didn't involve consumer's financial institution in digital signature technology
- 4) optionally involved shared secret methodology for end-to-end authentication (in addition to digital signature authentication)

The interesting characteristics is that the consumer financial institutions considered that they operate a consumer service business primarily and that electronic financial transactions are secondary.

While the technology demonstration may not have involved the consumer's financial institution in digital signature authentication, in consideration for migration to any sort of production operation, the consumer service nature of the business required that the financial institution be able to interact with the consumer with respect to their digital signature, i.e.

Aads

- a) this was not related to the consumer's financial institution performing digital signature authentication on electronic transactions
- b) this was related to the financial institution believing it is a consumer service operation and being able to support the consumer executing a digital signed financial transaction on an account at the financial institution.

The net was that even if financial institutions didn't implement technology for verifying digital signed transactions, they still registered the consumer's public key and provided service support related to digitally signed transactions (i.e. the call center could answer questions related to digitally signed transactions against the consumer's account).

What then became obvious, was that once the service operation registered the consumer's public key in the financial account record (regardless of the reason that it was registered), it was no possible to implement AADS-based authenticated transactions. One scenario has the financial institution "WEB-enabling" their call center so that (nearly) every transaction that could be transacted via the call center could also be transacted via AADS, public key signed, WEB transaction.

The other aspect of this was that the account registration and customer support aspects for supporting digital signature transactions represent the majority of the infrastructure expense. The cost of infrastructures in support of doing digitally signed transactions is actually a small percentage what is required to provide account-based consumer support infrastructure.

With respect to #4, the financial infrastructure eventually realized for production operation that they had support both a consumer public key in the account record (the service nature of the business required it, even if the technology aspect of transaction processing didn't) and a consumer shared-secret. From the infrastructure cost standpoint, registration, recording, updating, maintaining, servicing two different fields with all the associated call center support screens

Aads

associated with the field maintenance as well as being able to answer
r
questions when things went wrong.

The net is that AADS is a methodology that can be used to optimally upgrade existing authentication business processes while optimally integrating into existing account-based business process methodologies.

CADS approaches have been demonstrated to be useful in upgrading existing environments that lack authentication and account-oriented operations, especially when no prior business relationship may exist

[illegible]

aadsstraw

AADS Chip Infrastructures

Basic AADS chip strawman is a single function EC/DSS digital signing chip that is:

- * high integrity
- * tempested
- * immune to all known chip card attacks
- * true random number generator
- * can generate ECC key pair in <1sec
- * on chip ECC key pair generation
- * private key never leaves the chip

It can be configured as an independent hardware token or embedded in other devices:

- * contact chip card
- * contactless chip card
- * ring
- * watch
- * PDA
- * cellphone
- * USB token

The basic functions supported are:

- * PKCS #11 EC/DSS digital signing
- * PIN/Biometric initialization
- * PIN/Biometric activation
- * key pair generation
- * export public key

Normally the digital signing function is performed on some message that is associated with some identifier; account number, userid, employee ID, or other. The identifying information, formatting the message, and computation of the SHA-1 (FIPS-180) secure hash of the message is assumed to be performed by some supporting personal computing device (personal PC, cellphone, PDA, etc).

Non-personal Computing Devices

In applications involving non-personal computing device applications (point-of-sale merchant devices, employee building entry devices, etc), a "stand-alone" AADS chip (not operated in conjunction with a

aadsstraw

personal computing device like a PDA or cellphone) will require additional function to supply the ID information (account number, userid, employee id, chip id, etc) that is part of a digital signature authentication function.

In the case of personally owned computing devices, they can be relied on to provide the appropriate ID for the specific application requiring authentication.

For non-personally owned devices, the ID information would need to be provided directly by the chip. The non-personally owned device would

- * read-ID information from the AADS chip strawman
- * create message with ID information
- * compute SHA-1 of the message
- * PKCS#11 write hash to the AADS chip strawman
- * PKCS#11 read DSS signature from the AADS chip strawman

In order to support this business process, load-ID and read-ID functions are required.

There are multiple ID architectures possible:

- * single load-ID operation that is latched so that it can only be executed once. This ID would either be
 - 1) business process unique ID ... limiting the chip to a specific "ID" related function
 - 2) chip unique ID ... allowing the chip to be used in multiple different business processes, but requiring the business process to map the chip unique ID to a business process specific ID

An example might be an employee ID for building and corporate data process access. Either 1) the actual employee ID is loaded into the chip ... or 2) a chip unique ID is loaded and the employee access would map a card unique ID into a employee ID.

- * multiple ID slots that carry a "tag" identifying the associated use. Each slot could be latched so that it could only be initialized once.

This would more easily allow multiple application specific IDs to be carried in the AADS strawman (as opposed to relying on card specific

aadsstraw

ID and the application mapping the card ID to an application specific ID). This requires that the read-ID function supply an application specific tag to select the ID-slot to be read. The load-ID function would specify a ID-tag and ID-value and the card would return slot not available if there are no unallocated slots.

AADS strawman in conjunction with personal computing device (personal PC, embedded in personal watch, PDA, cellphone):

base	- digital signing
AADS	- PIN/Biometric initialization
chip	- PIN/Biometric activation
	- key-pair generation
	- public key export

incremental AADS chip function for use in conjunction with non-personal devices (like merchant point-of-sale, building access, etc).

incremental	- load/write-ID
AADS	- read-ID
chip	

Offline Purse Applications

The multiple-slot load-ID and read-ID functions could be extended for simple offline purse applications if the security issues could be worked out (and there was sufficient business justification).

First, some specific "non-latched" slots would be needed so that the load/write-ID function could not only initialize an unused slot .. but be used in subsequent updates to the same slot.

aadsstraw

The current typical offline purse application has almost all the logic in the reader and assumes little or no capability in the chip (other than allowing a value to be read and written). A slight expansion of this capability is Mondex and GSM applications where there is a infrastructure-wide shared secret in every card and the chip performs encryption.

The simpler offline purse applications have the infrastructure shared secret located in the reader and the card/chip is only used to carry the current (encrypted) value for the card. All the readers are assumed to be the trusted entities and therefore this application violates almost all of the strong AADS authentication guidelines.

The only relationship between AADS authentication applications and offline purse applications is that they both use chip technology.

AADS Strawman Card Management

The AADS Strawman chip/card management provides for a certified audit trail that shows a strong binding between:

- * assurance level of AADS chip
- * public (& private) key
- * account identifier
- * entity

In leveraging the existing debit card business process, the entity binding uses the "card" activation process where the card/chip is mailed to a specific address, the recipient initializes the PIN/biometric information, the card/chip is then used in conjunction with other authentication information for an activation transaction.

A slight modification to this business model is the card/chip mass-mailing. In this situation there is not a predefined binding between an account and any entity; just:

- * assurance level of AADS chip
- * public (& private) key
- * account identifier

aadsstraw

A recipient of such a mass mailing uses the card/chip in an activation process, but has to provide all the entity identity information at time of activation. This might be possibly used by Internet Service providers to simplify acquiring new customers. The mass mailing would include both (a CD-ROM) software and a card/chip. The customer would use the card/chip as part of the account activation with the service provider ... and at the same time provide sufficient detail such that the account use can be billed for.

Security Concerns & Issues

Denial of Service Attack

There is a security and/or denial of service attack with respect to all initialization functions

- * PIN/Biometric initialization
- * key pair generation
- * load-ID

The two approaches to handling the problem is to either

- 1) latch the functions so that each can only be performed once
- 2) requiring additional/re activation and/or authorization code for subsequent operations after the first

The issue is whether an unauthorized entity can force a value reset or a new value load. Single-time latching is used in conjunction with chip authorization (i.e. the chip is only activated for application use after all initialization functions have been performed).

The problem with multiple initialization and/or reset functions is that they become a point of attack and the process must be carefully evaluated.

Also, in the AADS card management process there is an audit trail binding the public/private key pair to a specific card at a known assurance level, as well as to some entity that the card has been issued to. Subsequent generation of a new key pair destroys that binding. For the mass distributed AADS strawman, it is probably less

aadsstraw

costly to redistribute a brand new chip (with audit trail binding) than it would be to establish an audit trail binding for an existing card that has had its key pair regenerated..

AADS Replay Attack

One form of attack is to record the message being authenticated along with the associated digital signature and retransmit the same information repeatedly. To forestall this form of attack, all AADS defined messages have field that contribute to making each message unique. The X9.59 AADS message defines in the message the account number, the date/time, and an account transaction sequence number.

For an AADS employee building access infrastructure, the badge reader needs to create a unique message (to be signed) for each operation. This could include the date/time, the badge reader ID number, and an incrementing sequence number in each message that was hashed for signing. Since no two messages would ever be the same, it would not be possible to do a stealth recording of an access transaction and then at a later time reply the recorded digital signature value to gain access (since no message is ever repeated, no hash will ever be repeated, and therefore no replay of a recorded digital signature will result in a valid authentication).

Random Number Requirement

SHA-1 (FIPS-180) is the standard secure hash for a message or document and is 20 bytes in length.

The standard RSA digital signature is to encrypt the SHA-1 value with the private key resulting in a 20-byte encrypted value.

One of the issues in digital signatures is to have sufficiently random information for possible slight variations on a message or document. To meet this requirement with a RSA signature, the message or document format typically includes a "Nonce" which has been defined as a (20-byte) random number included in the body of the message.

aadsstraw

The DSS (FIPS-186) approaches this problem differently, it defines that a random number is used in the signing calculations. The DSS digital signature (encryption of the 20-byte SHA-1 with the private key) results in two 20-byte numbers. Note that the transactions are the same size (whether the 20-byte random number is added to the body of the message or the digital signature contains a second 20-byte number).

In the past, card-based digital signature techniques have tended to use RSA signatures since the card chips haven't had true random number capability. The assumption was that the computing device that was generating the message for digital signing was more powerful and could reliably generate a random number included in the body of the message, before calculating SHA-1 hash for passing to the card for the digital signature functions. One of the downsides of this approach is that "public", untrusted readers could fail to generate a true random number and mount an attack on the card's private key by passing it hash values of messages that didn't have the appropriate random values.

The AADS chip strawman requires a chip capable of true random number generation and the use of DSS (FIPS-186) digital signature process to eliminate this attack. Except for one or two exceptions, none of the current card chips meet the requirement for true random number generation.

Hardware random number capability is also integral to implementations that resist some current chip card attacks.

RSA & ECC Strength

A couple years ago the formula for comparing RSA and ECC key strength was:

RSA - $10^{**}(\text{sqrt}(N))$
ECC - $10^{**}(N/4)$

where N is the number of bits in a key. RSA key of 2048 bits yields a value of $10^{**}45$. An equivalent ECC was 180bits (i.e. $10^{**}(180/4)$). Recent advances with number field sieve claims that RSA strength is

aadsstraw

reduced to

$$e^{*(1.9 * (\ln(N)^{(1/3)} * (\ln(\ln(N)))^{(2/3)}))}$$

Current RSA keys would have to be hundreds of times larger to give the same strength as a 2048-bit RSA key prior to the number field sieve work.

At the same time, SITI has made significant advances in enabling significantly stronger fields for practical public key use (compared to the default standard ECC field of a couple of years ago).

Key lengths less than 128 bits are not recommended (regardless of the field strength) because of the possibility of rapidly trying every possible key combination in a brute force attack.

Trusted Computing Devices

One of the fraud opportunities is for compromising a "non-personal" point-of-sale device, especially in financial transactions. A merchant device displays a financial transaction involving a sum of \$20. The hash sent to the AADS chip for signing is actually for a transaction involving \$100. The minimal AADS strawman has no personal input and display function and so the owner must rely on the merchant device and authorize the transaction.

The most general solution to this problem is for an person to always do their transaction with a portable personal (trusted) computing device that contains its own input and display facilities (like a PDA, cellphone or watch). The merchant transmits the whole message to be signed to the PDA, the PDA calculates the hash and executes the PKCS#11 signing function to the embedded AADS chip. The PDA (or cellphone) displays the message for the owners approval (rather than relying on a possibly untrusted merchant device to display the value being authorized).

The less desirable solution is to have certified point-of-sale devices

aadsstraw

that are tamper resistant or at least tamper evident along with some sort of online verification regarding correct operation (i.e. there is very low likelihood that the point-of-sale device has been tampered with such that the transaction value displayed is different than the transaction message hash that gets signed.

A similar case holds for input activation functions that aren't "on-card". An example is a chip requiring a PIN value for correct operation. If the chip doesn't have a "on-card" pin-pad, some external pin-pad is relied upon for entering the PIN value which is then transmitted to the chip. If the input device is not part of the card or a personally owned PDA or cellphone, then there is the question can the PIN-pad be trusted (i.e. has it been modified to collect all PINs entered and save them for future possible use).

In non-private areas, the certification and trust for non-personally owned input and display devices is a security and integrity issue.

Shared Secret Attacks (offline purse/stored value)

Many of the current chip card applications assume some sort of distributed offline operation which requires an infrastructure shared secret for authorized operations between chip cards and other facilities. These can be merchant point-of-sale devices, electronic vending machines, or transit system electronic turn-styles.

In the simplest form, the card may only contain the current card balance in encrypted form.

A offline stored value device

- 1) reads the encrypted value from the card
- 2) decrypts using the infrastructure shared-secret (common to all point-of-sale devices in the same infrastructure),
- 3) updates (adds/subtracts) the value,
- 4) re-encrypts the value
- 5) writes the updated, encrypted value back to the card

Since lots of different devices will all be operating against the sa

aadsstraw

me

cards (and the same encrypted values), all devices in the same infrastructure have to share a common secret in order to be able to decrypt values that had been encrypted by other devices.

For infrastructures with shared secret contained in both the card chips and the reader chips, either a card or a reader can be attacked to extract the infrastructure shared secret and put the infrastructure at risk. In the implementations where the shared secret is only contained in the reader, then a reader must be obtained for an attack to put the whole infrastructure at risk.

Also, the certificate and trust of these offline, purse devices is more significant than for the point-of-sale AADS operation (especially given the lack of any sort of online audit trail). The frequent response is that the amounts at risk in the offline stored-value are less than the amounts at risk in online payment transactions).

Incremental enhancement to the offline purse application defines a authenticated transaction between the card and reader. This typically takes the form of a second shared secret that all readers and cards understand which is used to (DES) encrypt all traffic between cards and readers. Only cards and readers that shared the same infrastructure shared secret will be able to inter-operate since (DES) decryption is required to correctly execute. This becomes an additional infrastructure point of attack.

Appendix

Radius References

>From the originators of RADIUS:

<http://www.livingston.com/tech/technotes/500/index.html#RADIUS>

Free Radius (1.6) Source:

<ftp://ftp.livingston.com/pub/1e/radius/>

aadsstraw

From:

page, select "Term", and then on the Term page, select the acronym RADUIS. This will give the list of all RADUIS RFCs. The individual RADUIS RFCs can be viewed by selecting the ".txt=" entry for that RFC.

004080-92022209

Account Authority Digital Signature
in support of
High Integrity Business Processes

One of the inhibitors to the deployment of high integrity business processes has been the lack of strong authentication infrastructure (a chain is no stronger than its weakest link).

Account Authority Digital Signature is a practical application of digital signatures for strong authentication which is opening up

aadsstraw

practical high integrity business processes.

Account Authority Digital Signature has investigated a combination of methodology and best practices approaches to strong authentication.

In part, this recognizes that strong authentication is just a part of (or preliminary to) a much larger business process.

As a methodology approach, Account Authority Digital Signature looks for existing authentication business processes (that may use passwords, PINs, and/or other forms of shared secrets) and upgrades them with digital signature technology.

As a best practices approach, Account Authority Digital Signature has looked at:

- * digital signature technology
 - best of breed digital signature technology like SITI's elliptical curve cryptography
 - AADS chip strawman providing optimal, highest integrity hardware token for digital signature processing
 - . public/private key generated in chip
 - . private key never divulged
 - . immune to all known smartcard attacks
 - . true random number generator
 - . tempest
 - . pin activation migrating to biometric
 - . aggressive design and volume pricing
 - form factor neutral deployment
 - . card
 - . ring
 - . cellphone
 - . PDA
 - . watch
 - . USB
 - . contact and contactless
- * digital signature authentication
 - session authentication
 - . i.e. upgrade RADIUS for digital signature
 - transaction authentication

aadsstraw

- . X9.59 for all account-based transactions; preserves integrity of financial infrastructure with just a digital signature.
- document authentication

- * digital signature binding
 - AADS hardware token issuing process providing optimal cost/benefit
 - binding
 - . known assurance level of hardware token
 - . public key
 - . entity or attribute binding to be associated with digital signature use
 - . account
 - privacy neutral
 - auditable key and binding registration process
 - . unique public key per application
 - . same public key for multiple applications

- * parameterized risk management based on audit trail associated with provable digital signature bindings; on per transaction basis able to consider:
 - assurance level of hardware token
 - token, pin or biometric activated
 - binding process
 - registration process
 - strength of specific ECC curve and field

The fundamental authentication advances provided by the Account Authority Digital Signature effort opens up significant new practical opportunities for establishing high integrity business processes across all business operations and industries.

AADS as a fundamental, ubiquitous, optimal "horizontal" authentication building block across all industries and applications:

- * access to financial services & records
- * account-based financial transactions (X9.59)
 - all environments from point-of-sale to WEB merchant servers
 - all transactions types, debit, credit, atm, echeck
 - upgrade for existing PIN/DES-based ATM cards
- * session establishment for connection to Internet Service Providers
 - leverage Internet standards like RADIUS for ubiquitous deployment

Aadsbrnd

AADS Brand Conventions

AADS always signs an AADS computed SHA-1 (on the data transmitted for signature, even if the transmitted data is a SHA-1). The issue is an y future circumstances where the issues is raised on whether the raw data stream was offered to the consumer's AADS environment or not (did the consumer at least have some sort of opportunity for viewing what was signed). A "double" SHA-1 leaves no ambiguity regarding whether the consumer's AADS device was presented the raw data stream, computed the SHA-1 and signed it or whether the consumer's AADS device was presented a precomputed SHA-1.

The AADS signature is always DSS (a new random number is computed for every digital signature operation). Even consecutive signing of the same exact data will always result in different DSS results.

Basic AADS chip functions

Generate key-pair

This operation is normally "latched" so that it is only performed once per chip. The sole caveat is this latch may

be reset if the chip has been zero'ized. When latched, subsequent execution returns invalid function

Export public key

The private key is never available outside of the AADS signing environment. However, the public key needs to be exported after initial generation. This operation may be optionally latched (see brute-force attack considerations). When latched, subsequent execution returns invalid function.

Perform DSS signature

A data stream is provided to the AADS signing environment, which performs a SHA-1 on the data stream and then signs the

Aadsbrnd

calculated SHA-1. Procedures for doing streaming SHA-1 calculations need to be verified (i.e. calculating SHA-1 on data stream much larger than local available memory). There may optional service enhancements in some AADS devices that provide additional operation as part of signing a data stream.

m.

PIN-activated AADS devices

Initialize PIN

Personalization services may ship an uninitialized PIN card to a consumer. There can be a combination process where the consumer both initializes the device PIN for the first time and activates use of their device with their service provider and/or financial institution.

Enter PIN

For PIN-activated AADS devices, entering a PIN will enable the correct operation of the digital signature function. To address brute-force offline attacks, the digital signature function will always return a reasonable result, regardless of whether the correct PIN has been entered, an incorrect PIN has been entered or no PIN has been entered. This is an issue since normal range of PIN values are four digits which is readily susceptible to offline brute-force attack on a stolen AADS device (typically approx. 2^{10} possible values).

Biometric-activate AADS devices

Initialize biometric

similar consideration to "Initialize PIN"

Enter Biometric

Similar to Enter PIN. For biometrics with $>2^{100}$ possible values are less prone to brute force offline attacks so some of

Aadsbrnd

the PIN attack considerations might not apply.

PIN Offline Brute Force Attack Considerations

A stolen PIN-activated AADS device is susceptible to brute-force offline attacks (especially when the range of possible values is $<2^{100}$). To thwart this attack, there should be no obvious differentiation between digital signature results using incorrect or correct PINs (i.e. digital signature operations when activated with an invalid PIN should be invalid in non-obvious ways).

Since DSS is being used, even consecutive signatures on the same data using valid PINs are not the same (so all signature results should be different regardless of what PIN is used).

One way that an attacker can distinguish valid signatures from invalid signatures is if they possess the public key and can directly verify the signature. To thwart this mechanism, infrastructures may choose to not make the public key readily available.

A simple method for generating an apparently good signature when a bad PIN has been entered is to modify the raw data as its SHA-1 is being calculated and then generate a valid signature using the private key. This can be done in a random way and/or in a very predictable way (see enhanced X9.59 services).

Enhanced X9.59 AADS Services.

To support future Internet and POS environments a version 1 X9.59 signed format is defined (version 0 being the original X9.59 ASN.1 encoded signed format). Version 1 X9.59 signed format uses all the same fields as version 0 but with XML-encoded (with FSML deterministic encoding considerations).

When the raw XML X9.59 data stream is transmitted to the consumer's AADS signing device for digital signing, the AADS signing device may

Aadsbrnd

recognize the object being signed and perform special functions.

A preliminary format for the XML encoded signed object can be found at

in section "Sample X9.59 tagged format" (last section in the web page).

The X9.59 signed object data stream is defined as being from the "<" (less than) of the <x9.59v-doc> tag to the ">" greater than of the </x9.59v-doc> tag (not including the trailing newline character or i

t
may be easier to just include the trailing newline character).
End-of-line within the body of the X9.59 signed object is a single new-line character (SHA-1 treats the data a single sequential bit-stream regardless of any textual meanings and/or delimiters).

Added value X9.59 features in this environment can always overlay some tag field value with a value stored in the consumer's AADS device (or optionally insert a field value only when the supplied value is null). Fields that this might be done for are:

- * prc_c
- * date_e
- * luid

The enhanced x9.59 services can support the saving of x9.59 field values and/or management of x9.59 field values. This will require spare memory in the device for field values. This will allow an AADS device to be used for X9.59 financial transactions in environments where it is not necessary to know the consumer's account number (and/or expiration date).

Another possible enhanced X9.59 function is for the AADS device to keep track of transactions executed by supplying the luid field (and incrementing the value after each X9.59 signature operation).

Any fields supplied and/or overlayed in this manner by the enhanced X9.59 functions need to be returned as part of the signature results in the perform signature response.

Enhanced X9.59 functions when attacked

Aadsbrnd

As part of infrastructure support to thwart brute-force attacks on stolen PIN-activated AADS devices, enhanced X9.59 services can offer specific operations. Given that the other forms of attacks are thwarted, that only leaves the attacker with attempting valid online transactions. While the basic AADS process for thwarted attacks is to return a signature on data other than provided, the enhanced X9.59 services can codify the way the data has been modified, given the online service hints as to attack being in progress.

In the X9.59 mapping to 8583, the X9.59 object_type field is never transmitted since it is always assumed to be a fixed value for an authorization request. When the online service goes to recreate the original signed object and verify the signature, it always plugs in a fixed value into the object_type field before calculating the SHA-1 on the reconstructed object.

X9.59 enhanced services can always choose to modify this specific field using a proscribed convention when a valid PIN has not been entered. When the object is reconstructed, the signature will fail because the object actually signed was not a bit-for-bit duplicate of the reconstructed object.

A possible modification convention can for enhanced X9.59 services in an AADS device:

valid PIN:	OBJECT_TYPE
no PIN:	OBJECT_TYPE+1
invalid PIN:	OBJECT_TYPE+2

The online service, when an invalid signature is encountered, can modify the reconstructed data with the different possibilities and attempt to re-verify the signature.

Sample x9.59 Tagged Format Section

Sample X9.59 Tagged Format

Aadsbrnd

X9.59 signed elements in a sample tagged format:

```
<x9.59v-doc>
<std_ver>nnn...
<object_type>nnn...
<paycode>nnn...
<prc_c>nnn...
<luid>nnn...
<prc_m>nnn...
<paydata_c>nnnn.nn:nnn
<date_s>nnn..
<date_e>nnn...
<shs>hhhhh...
</x959v-doc>
<sig>hhh....:hhh....
```

nnn...

is numeric data

hhh...

is hexadecimal representation of binary data

a colon is used to separate amount and currency type in paydata

-c

a colon is used to separate DSS r and s values

<shs>

is the SHS of the order detail document

<sig>

is the DSS signature of the tagged elements

Rachip

AADS Chip Strawman

Registration Authority (now called PRiMR)

The purpose of the AADS Chip Strawman PRiMR is to help raise the overall risk management of the authentication infrastructure. The emerging chip technology represents a significant improvement in the assurance level of card-based authentication mechanisms (especially compared to existing magstripe based infrastructures).

This emerging technology assurance level is so high that issues of counterfeit chips start to become an important factor. One of the issues that the AADS Chip Strawman will address is the issue of counterfeit chips (possibly counterfeits that have backdoors introduced).

The AADS Chip Strawman PRiMR is viewed as a layered set of features that meet a range of business requirements. The business operations are viewed as:

- 1) trusted anonymous chip-cards
- 2) trusted personalized chip-cards
- 3) trusted personalized chips-cards with activation

The common characteristics of

- * tempested
- * immune to all known smartcard attacks
- * pin-activated (migrating to on-card biometric)
- * tamper-evident with zeroization.
- * public/private key generated on the card
- * private key is never divulged
- * public key can be exported
- * only function supported is EC/DSS (elliptical curve version of FIPS186)

Some early results is that an AADS-only chip can be do'able in as little as 20,000 circuits (by comparison the Intel 486 was over four million chips and more recent chips are significantly larger). Both ECC public/private key generation and EC/DSS signature signing can be done on the order of 10 milliseconds or less.

Basic PRiMR Function and Requirements

Rachip

The most basic AADS Chip Strawman PRiMR function is establishing the binding between a public key and chip characteristics. This requires at least secure audit trail of a chip and the associated assurance characteristics of that chip. A public/private key-pair are generated in a controlled environment and the public key is registered with the secure audit trail of the chip and the associated chip assurance characteristics. This is the most basic AADS Chip Strawman PRiMR function.

In effect, this basic function can be viewed as establishing the initial chip public key as the chip's serial number; i.e. in addition to various cryptographic operations, the public key can be used as if it were the chip serial number. Operations that might be associated with correlating a chip serial number with a chip manufacturing history or the chip's assurance level are driven using the chip's public key (and/or cryptographic operations involving the chip's private and/or public key).

This level of function can be used things like:

- * chip card mailers, an example would be in conjunction with AOL CDR inserts that allow people to establish an AOL account. The card can be used for establishing an AOL account and then subsequent authentication for use of that same account requires the card that was used to setup the account.
- * chip manufacturers that want an inexpensive method to address the copy-chip and chip grey market. The AADS strawman circuits would be included in a secure portion of a standard chip product and would operate in the same manner as the AADS chip. In effect, the AADS public key becomes the serial number of the chip and the manufacturer can leverage the AADS PRiMR infrastructure to validate a chip.

In numerous discussions with various parties that are authentication stakeholders, the "anonymous" card for mail inserts was a stated requirement (can validate the assurance level of the authentication mechanism without having to validate the identity holding the authentication mechanism).

Rachip

The second scenario came about during discussions with various a couple companies that are potential for manufacturing the AADS strawman chip. We wanted to be able to trace a high assurance, audit trail back through the chip design and manufacturing. After some detailed discussion, they expressed a very strong interest in being able to use the AADS high assurance process for all of their chips.

One proposal is that a AADS chip strawman PRiMR be installed at the chip manufacturing plant which is operated and overseen by FDC. The standard chip test and burn-in process would have the AADS public/private key generation added, along with exporting the key to the PRiMR database. The secure binding between the chip public key (aka chip serial number) and the chip assurance characteristics then occurs at the chip manufacturing plant.

This process is then available for use with the AADS authentication chips (that are targeted for chip cards) as well as the rest of the chips manufactured in the plant. Part of the motivation with having FDC responsible for the PRiMR is the recent uproar with having serial numbers in Pentium-III chips. FDC is already an acceptable party which keeps mappings between individual characteristics and authentication mechanisms.

The characteristic of the this PRiMR database includes pointers to chip part number, chip lot/batch number, chip lot/batch processing audit trail, and ECC algorithm. The chip part number, chip lot/batch information, and ECC algorithm information is used in establishing the chip assurance level characteristics. This is also part of the support for parameterized risk management since as various new exploits appear, they can be evaluated against specific chips and/or algorithms and the associated assurance level adjusted as needed.

The "anonymous" chip card has an uninitialized PIN capability. The person receiving the card will first initialize the PIN and then use the card in an online registration process (for instance establishing an AOL account and registering the card's public key as the authentication mechanism for the account).

Personalization PRiMR Functions and Requirements

Rachip

The personalization PRiMR functions and requirement build on the basic functions. This will be deplorable in two ways:

- a) basic and personalization functions combined in single operation
- b) personalization receives batch of chips from foundry along with information from the foundry PRiMR (public key and chip characteristics)

In the case of "a", the basic function still needs to be executable independently without requiring the personalization function (for support of "anonymous" chipcards as part of mailers and inserts).

The personalization operations include:

- * correlating the personalization process with the AADS chip "serial number" (aka chip's public key)
- * potentially embossing in a combo chip/magstripe card
- * establish the card PIN activation number
- * mail/deliver the card
- * under separate cover, mail/deliver the card PIN
- * deliver the card's public key and personalization information to the organization initiating the personalization request

The party receiving the card uses an online "card" activation process (in a manner similar to the AOL registration example) to indicate that they have received the card and can activate it. The online card activation process can be as simple as signing a dummy message containing the card's public key. The activation process might also contain the transmittal of additional authentication information via an encrypted channel (i.e. browser SSL or IPSEC). The card activation event is also transmitted to the organization initiating the personalization request.

Some additional optional chip-card operational characteristics:

Rachip

For non-anonymous PIN cards, there may be a function to change the card's PIN activation code under controlled circumstances (i.e. using the existing PIN code to enable the function to change the PIN). For the anonymous PIN card, the one-time PIN definition process must be executed before AADS signature functions are active.

For chip-cards that have been built with biometric activation, the initial PIN code is only used to activate the biometric initialization function. Once the biometric initialization function is performed, the initial PIN code is no longer usable and biometric card activation is required. This is analogous to the process where the card owner can change the PIN-activation code (making the previous PIN-code invalid).

Observations

At a very high level, the AADS strawman PRiMR combines some of the characteristics of magstripe PIN processing with some of the characteristics of the online AOL account registration with additional features to track and record the assurance level of the chip and associated audit trails.

Given that one of the objectives is to be able to provide an audit trail as to the assurance level of the chip (and that, in fact it is not a copy chip with built in back doors), the integrity and auditability of the design, development, and implementation of all the processes and components must be at the highest assurance level practical.

The critical components of the process

- * assurance level of the design and manufacturing of the chip
- * handling of the chip between the time the chip is manufactured and the time its public key is established (as the chip serial number) and recorded. Be able to have audit trail tying chip batch/lot number, chip design, manufacturing up until the time the chips have their

Rachip

public/private key generated and the public key registered in the database (along with pointers to the audit trail)

- * database recording the chip's public key (aka chip serial number) and mapping the public key to the characteristics of the chip

- * any associated information that is added to the chip record (for instance identity information that may occur as part of the personalization process)

- * the security and integrity of the PRiMR database(s)

- * the security and integrity of the operations updating the PRiMR database(s)

- * the availability of the PRiMR database(s)

Viewing the opportunity another way, the current magstripe authentication card is at much lower assurance level than many of the related processes in the financial infrastructure. The emerging chip technology has the potential of increasing the card component assurance level to be much higher than many of the other processes (especially card related) of the financial infrastructure. Furthermore, the card (& chip) business appears to becoming an increasing commoditized operation.

The AADS strawman PRiMR is part of an end-to-end solution that increases the assurance level of the rest of the card infrastructure to be comparable to that of the emerging chip assurance levels. This creates a much higher value proposition and moves the card from being a commoditized to being part of an overall risk management solution for the financial industry.

PRiMR Database Sizings

There are two types of database designs, one with the initial public key registration a separate function from the personalization information and one where the functions are combined.

In the first case, the separate public key registration handles high burst transactions from test & burn-in assemblies that are also activating the key generation function. The key generation time is approximately 10 milliseconds or less. The transaction insert rate is

Rachip

proportional to the test, burn-in & key generation elapsed time per chip times the number chips that are processed simultaneously. Chips are manufactured in wafers. There is possibility of between 300 and 3000 AADS chips per wafer process. The test, burn-in and key generation is likely to be in the multiple minute range, so bursty transactions could be in tens per minute or in the single digits per second.

It is initially believed that the combined personalization process (with embossing and other characteristics) will have bursty transaction rates that are lower than the separate manufacturing process.

In the personalization part, when the processes are separate, the personalization database must be prepared to accept a batch load of all keys that come in with a chip (or chip-card) shipment, along with the batch/lot numbers in the shipment and the associated assurance characteristics and handling audit trail.

For the actual personalization phase, the personalization database can expect a batch load of all the requested personalization information. As individual chip/cards are personalized, the public key and assurance information must be tied to the personalization information.

For the online card activation phase, an online webserver is necessary that can interact with a customer browser applet that verifies the card information and appropriately executes the card activation validation and processing function.

There are three possible design points for the PRiMR database, that supports 10 million chips, 100 million chips, and a billion chips.

The expected peak card activation load on the webserver has yet to be estimated, although it is likely to only be on the order of a few transactions per second.

The functions supported by the PRiMR

- * key, assurance, and audit trail input transaction (both batch and "interactive")
- * personalization information input transaction

Rachip

(both batch and "interactive")

- * possible cross-connecting the key and personalization transaction primarily "interactive"
- * webserver card activation transaction primarily "interactive"
- * personalization, key, assurance and card status export both batch and "interactive"
- * individual personalization, key, assurance, and card status query transactions

004080-92000000